Treball final de grau

GRAU DE MATEMÀTIQUES

Facultat de Matemàtiques i Informàtica
Universitat de Barcelona

ELLIPTIC CURVES AND A THEOREM OF GAUSS

Autora: Karuk Andriana

Director:	**Eduardo Soto**
Realitzat a:	**Departament de Matemàtiques i Informàtica**
Barcelona,	**18 de gener de 2019**

Abstract

Just like in life, in mathematics many times we find ourselves seeking for the unknown as are the solutions of an equation. In our case instead of focusing on the solutions we would rather know how many options there are, and so how many solutions we can have in a given equation.

The aim of this work is to study some of the properties of elliptic curves, as well as some additional theory related to the p-adic numbers and idèles. Moreover, we will see how a perfect combination of it all can helps to find out how many solutions there are of an elliptic curve over a finite field with some additional conditions.

Resum

En la vida, igual que en les matemàtiques moltes vegades busquem allò desconegut com són les solucions d'una equació. En el nostre cas enlloc de centrar-nos en les solucions, mirarem quantes opcions podríem tenir i per tant, quantes solucions hi hauria d'una equació donada.

L'objectiu d'aquest treball és estudiar algunes de les propietats de les corbes el·líptiques i introduir alguns conceptes i resultats en els nombres p-àdics i els idèles. A més a més, veurem com combinant-ho tot podem trobar quantes solucions hi ha d'una corba el·líptica sobre els cossos finits amb algunes condicions afegides.

2010 Mathematics Subject Classification. 14H52, 11M41, 11E95

Acknowledgments

First of all, I would like to express my gratitude to my teacher Eduard Soto, for his dedication, support and patience during these months. Thank you for discovering the elliptic curves for me, as well as their potential.

I would like to thank my friends, who have been by my side though this experience and have listened to me talk about my project almost every day.

Last but not least, I would like to give a special thanks to my parents, who always encourage and support me and who helped to pursue this goal. And to my grandfather, who is the reason I felt in love with Mathematics in the first place.

Contents

Introduction

Among the most remarkable theorems in the history of mathematics is Fermat's last theorem. Conjectured in 1637 in the margin of a copy of *Arithmetica*, unsolved until 1994 when Andrew Wiles came up with the proof that would help with the development of algebraic number theory as well as modularity theorem. Fermat's last theorem states that for n greater than 2 there are no three positive integers x, y, z such that $x^n + y^n = z^n$.

One can ask himself, what if instead of changing the exponent, we change the base field, will that make a difference? How many solutions are there in every field? Moreover, what if we consider different equations of the same degree and focus on how many solutions they have depending on the field? And so in our case, we set $n = 3$ and find ourselves working with a cubic plane curve , and our field of game will be a finite field $\mathbb{F}_p$, with p a prime.

In fact, Hasse estimated the number of solutions to a cubic equation over a finite field. But it was Gauss in the *Disquistiones Arithmeticae* who proved some special cases of Hasse's theorem. One of those cases is the curve in homogeneous form $x^3 + y^3 + z^3 = 0$ that appears in the Gauss theorem that gives the amount of solutions of this curve over a finite field $\mathbb{F}_p$ depending on the prime p.

As a matter of fact, the equation in the Gauss theorem is called an elliptic curve, and those are the purpose of the study in this dissertation. We will start by giving a definition of an elliptic curve, and will study some of its main properties as well as Hasse's theorem itself. Concretely, we will deal with elliptic curves with complex multiplication with the intention of understanding in a deeper way the equation given, and to set the basis to be able to talk about how many solutions there are for an elliptic curve with complex multiplication in a finite field.

In order to achieve our goal, once we are familiar with the elliptic curves, we will move to the p-adic numbers which will help us to have a better understanding of idèles. Later on, we will introduce Hecke characters from an idèlic point of view. Through the reading we will find some results that help us find the amount of solutions of an elliptic curve.

We will assume previous knowledge corresponding to the subjects taught at University of Barcelona: Projective Geometry, Algebraic Structures, Algebraic Equations, Topology, Mathematical Analysis, Complex Analysis and Analytic Methods in Number Theory.

Chapter 1

Elliptic curves

Even thought nowadays elliptic curves are mainly used in cryptography[1], their mathematical properties have been studied for many centuries now, and are used a lot in number theory.
The name of "elliptic" comes from the fact that these curves were a result of the problem of finding the arc length of an ellipse.
In our case we are going to introduce elliptic curves and study some of its main properties. In the first two sections we will be talking about elliptic curves given by a special Weierstrass equation, since any elliptic curve can be expressed in a Weierstrass form. Moreover, we will talk about a special case of elliptic curves, those with complex multiplication therefore we will introduce the ring of endomoprhisms of an elliptic curve.
Furthermore, we will focus on some important results for elliptic curves over complex numbers as well as a finite field. In fact, in the Gauss theorem we find an elliptic curve over a finite field.

1.1 What is an elliptic curve?

Definition 1.1. An *elliptic curve* E is a non-singular algebraic curve defined over a field K of genus 1 with a base point O, denoted by E/K.

Remark 1.2. We will not define genus for an algebraic curve but for plane curves, non-singular genus 1 curves are exactly non-singular curves defined by a cubic polynomial.

After a change of variables[2] every cubic plane curve can be described by the following expression

$$E: \ Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

in $\mathbb{P}^2$. Where $a_1, a_2, a_3, a_4, a_6 \in K$.

[1] Elliptic Curve Cryptography (ECC), a public key cryptography introduced by Neal Koblitz and Miller in 1985.

[2] See [7] , Chapter 1.3

It is a representation of an elliptic curve given by *Weierstrass equation* also called *general Weierstrass equation*. The base point is $O = [0 : 1 : 0]$ that is the point at infinity which we obtain when $Z = 0$.

Remark 1.3. From now on when talking about an elliptic curve we will relate it to the previous expression.

Definition 1.4. Let E be a plane curve over K. A point on the elliptic curve $[x_0 : y_0 : z_0]$ is nonsingular if and only if at least one of the partial derivatives $\frac{\partial F}{\partial x}$, $\frac{\partial F}{\partial y}$, $\frac{\partial F}{\partial z}$ is nonzero at $[x_0 : y_0 : z_0]$.

The following definition of a nonsingular elliptic curve is going to be used.

Definition 1.5. An elliptic curve is *nonsingular* if all of its points in $E(\overline{K})$, i.e. in the algebraic closure of K, are nonsingular.

Generally the Weierstrass equation is written in non-homogeneous coordinates. If we take $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$ then

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Definition 1.6. Given any field extension $L|K$ we can define the set of points of the elliptic curve E on L with coefficients a_i in K.

$$E(L) \ := \{(x,y) \in L \times L \ : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\}.$$

In what follows, the necessary conditions will be specified for the the Weierstrass equation to be an elliptic curve, i.e. nonsingular. Previously a new concept is introduced.

Definition 1.7. Given a field K and an elliptic curve E/K by the Weierstrass equation its *discriminant* Δ is given by the following formula

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

where

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6$$
$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$

Theorem 1.8. *The curve given by the Weierstrass equation is nonsingular if and only if* $\Delta \neq 0$.

Before moving on to prove the theorem 1.8 some necessary results need to be listed. First of all, the Weierstrass equation given over K by

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

can be simplified. Suppose $char(K) \neq 2$ and take the equation 1.2 to complete the square

$$\left(y + \frac{1}{2}(a_1x + a_3)\right)^2 - \frac{1}{4}(a_1x + a_3)^2 = x^3 + a_2x^2 + a_4x + a_6$$

substitute $y + \frac{1}{2}(a_1x + a_3)$ for $\frac{1}{2}y$. The result is a simplified equation

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \tag{1.1}$$

where

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6$$

Proposition 1.9. *If c is a nonzero element of a field K with $char(K) \neq 2$ then the plane curve*

$$y^2 = c(x^3 - \alpha x^2 + \beta x - \gamma)$$

is nonsingular if and only if $f(x) = c(x^3 - \alpha x^2 + \beta x - \gamma)$ has distinct roots in K.

Proof. First have a look at the infinity point $O = [0 : 1 : 0]$ and use Definition 1.4 to see that it is always nonsingular. Take the partial derivative at the infinity point

$$\frac{\partial F}{\partial Z}(0, 1, 0) = 1 \neq 0$$

so O is nonsingular and the curve is singular if there exists a point $[x_0 : y_0 : 1] \in \overline{K}$ on the curve that satisfies the following three equations:

$$\begin{cases} \frac{\partial}{\partial x}: & 0 & = & 3x_0^2 - 2\alpha x_0 + \beta \\ \frac{\partial}{\partial y}: & 2y_0 & = & 0 \\ \frac{\partial F}{\partial z}: & y_0^2 & = & c(-\alpha x_0^2 + 2\beta x_0 - 3\gamma) \end{cases}$$

The first two are equivalent to

$$0 = y_0 = f(x_0) = f'(x_0)$$

The third one is redundant, giving the extra condition

$$3f(x_0) - x_0f'(x_0) = 0$$

Therefore if x_0 is a root of f then the only candidates for singular points over $\overline{K}$ are $[x_0 : 0 : 1]$.

Such a candidate is singular if and only if x_0 is a multiple root of f. □

Let

$$f(x) = x^3 - \alpha x^2 + \beta x - \gamma = (x - r_1)(x - r_2)(x - r_3)$$

be a monic polynomial over K with roots in $\overline{K}$. With

$$\alpha = r_1 + r_2 + r_3, \quad \beta = r_1r_2 + r_1r_3 + r_2r_3$$
$$\gamma = r_1r_2r_3$$

The discriminant d of $f(x)$ is given by $d = (r_1 - r_2)^2(r_1 - r_3)^2(r_2 - r_3)^2$

Proposition 1.10. *Given a field K such that $char(K) \neq 2$, let d_r be the discriminant of the cubic polynomial $4x^3 + b_2x^2 + 2b_4x + b_6$. Then following notation of 1.1, $\Delta = 2^4 d_r$*

Proof. See [2] Chapter 3, Proposition 3.6. □

Proof theorem 1.8. Take the following homogeneous equation

$$F(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0$$

First study the points at infinity. If $Z = 0$ then $F(X, Y, 0) = 0$, so the only point at infinity is $O = [0 : 1 : 0]$. In the proof of Proposition 1.9 we have already seen that O is nonsingular.

Now suppose $P \in E$ and $P \neq O$. And taking non-homogeneous equation

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.2}$$

There are two different cases.

First suppose $char(K) \neq 2$. The equation 1.2 is nonsingular if and only if equation 1.1 is. And by Proposition 1.9 it is nonsingular if and only if its roots are distinct, so if and only if the $d_r \neq 0$. Using the Proposition 1.10 it is clear that when $char(K) \neq 2$ the curve given by the Weierstrass equation is nonsingular if and only if $\Delta \neq 0$

Now suppose $char(K) = 2$. The Δ reduces into

$$\begin{aligned}\Delta &= b_2^2b_8 + b_6^2 + b_2b_4b_6 \\ &= a_1^6a_6 + a_1^5a_3a_4 + a_1^4a_2a_3^2 + a_1^4a_4^2 + a_3^4 + a_1^3a_3^3\end{aligned}$$

In order to prove the desired result it is equivalent to see the curve given by the Weierstrass equation is singular if and only if $\Delta = 0$. Applying the definition 1.4 the Weierstrass equation 1.2 is singular if and only if there exists a $\overline{K}$ rational point $[x_0 : y_0 : 1]$ on the curve such that satisfies the following equations

$$\begin{aligned}\frac{\partial}{\partial x} &: 0 = a_1y_0 + x_0^2 + a_4 \\ \frac{\partial}{\partial y} &: 0 = a_1x_0 + a_3\end{aligned}$$

Suppose $a_1 = 0$. Then by one of the previous equations $\Delta = 0$ if and only if $a_3 = 0$ if and only if it holds that $0 = a_1x_0 + a_3$. It is enough to show that

$$\begin{aligned}y_0^2 &= x_0^3 + a_2x_0^2 + a_4x_0 + a_6 \\ 0 &= x_0^2 + a_4\end{aligned}$$

has a solution in $\overline{K}$. Choose $x_0 \in \overline{K}$ such that the second equation holds and substitute it into the first one and get $y_0 \in \overline{K}$ so that the first equation holds as well.

Suppose $a_1 \neq 0$. The derivatives give

$$x_0 = \frac{a_3}{a_1}, \quad y_0 = \frac{a_3^2}{a_1^3} + \frac{a_4}{a_1}$$

Once substituted in the equation 1.2 get

$$\frac{a_1^6 a_6 + a_1^5 a_3 a_4 + a_1^4 a_2 a_3^2 + a_1^4 a_4^2 + a_3^4 + a_1^3 a_3^3}{a_1^6}$$

where the nominator is Δ. So $[x_0 : y_0 : 1]$ found is a singular point on the Weierstrass equation if and only if $\Delta = 0$. So when $char(K) = 2$ the curve given by the Weierstrass equation is nonsingular if and only if $\Delta \neq 0$.

In conclusion, when the curve is represented by the general Weierstrass equation it is nonsingular if and only if $\Delta \neq 0$. □

Remark 1.11. It has been proved that a curve represented by

$$E: \ y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

is an elliptic curve if and only if $\Delta \neq 0$.

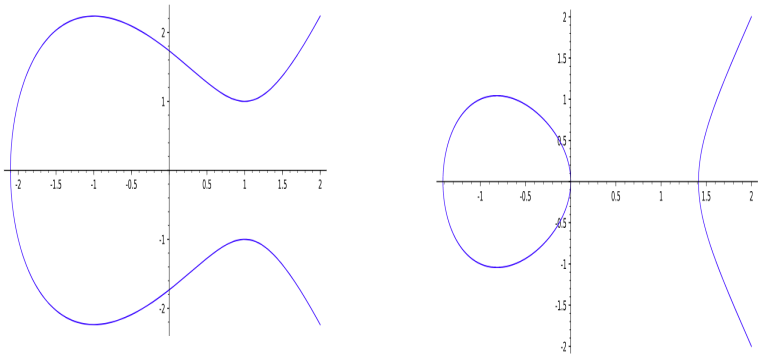
Definition 1.12. The *j-invariant* of an elliptic curve E in the Weierstrass form is the quantity j the defined as

$$j = \frac{\left(b_2^2 - 24 b_4\right)^3}{\Delta}$$

where

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1 a_3$$

and Δ is the discriminant of the curve.

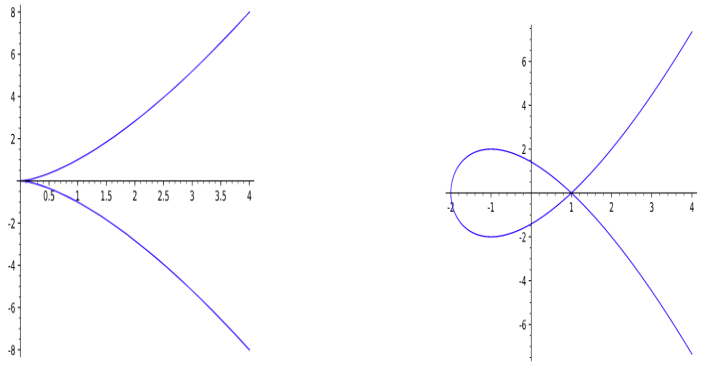


(a) $y^2 = x^3 - 3x + 3$, $\Delta = -2160$ (b) $y^2 = x^3 - 2x$, $\Delta = 512$

Figure 1.1: Elliptic curves

In the figure 1.1 we can visualize some elliptic curves. When the coefficients of an elliptic curve are real numbers, as in the figure, if the discriminant is negative then the roots are two complex conjugate roots and one real, as we can visualize in 1.1a. Contrarily, if the discriminant is positive there are three real roots, as exemplified in 1.1b. And so

depending on the amount of solutions we have two different representations.
In case of the singular curves represented in the Figure 1.2 we can find a node, as in 1.2a or a cusp as in 1.2b. We say that a singular curve has a cusp when there is one tangent direction, and that it has a node when there are two distinct tangent directions.



(a) $y^2 = x^3$, $\Delta = 0$ (b) $y^2 = x^3 - 2x$, $\Delta = 512$

Figure 1.2: Singular curves

Example 1.13. We would like to see that in fact $x^3 + x^3 + z^3 = 0$ is an elliptic curve.
As we have mentioned any cubic curve can be transformed into a Weierstrass form. We consider the map

$$\begin{array}{rccc} \theta: & \mathbb{P}_2 & \longrightarrow & \mathbb{P}_2 \\ & [X:Y:Z] & \longmapsto & [-12Z:-36(X-Y):X+Y]. \end{array}$$

For characteristic 0 or $\geqslant 5$ it is direct to check that it is a bijection. Indeed, assume that $12Z = 36(X-Y) = X+Y = 0$. Then $Z = 0$ and $X+Y = 0, X-Y = 0$ implies $X = Y = 0$.
The projective curve $C : X^3 + Y^3 + Z^3$ is sent by θ to $E : ZY^2 = X^3 - 432Z^3$.
Indeed, assume $x^3 + y^3 + z^3 = 0$. Then $[u:v:w] := \theta(x,y,z) = [-12z : 36(x-y) : x+y]$ and

$$\begin{aligned} wv^2 &= 1296(x^3 - x^2y - xy^2 + y^3) \\ &= 1296(x^3 - x^2y - xy^2 + y^3) + 432(x^3 + y^3) - 432(x^3 + y^3) \\ &= 1728(x^3 + y^3) - 1296(x^2y + xy^2) - 432(x^3 + y^3) \\ &= -1728z^3 - 1296(x^2y + xy^2) - 432(x^3 + y^3) \\ &= u^3 - 432w^3. \end{aligned}$$

In conclusion, through a transformation process of a cubic with a rational point into the Weierstrass form we obtain that $x^3 + y^3 + z^3 = 0$ is equivalent to $y^2 = x^3 - 432$ over $\mathbb{Q}$ in non-homogeneous coordinates . And we now want to verify that indeed it is an elliptic curve.
First of all we want to see that it is non-singular. As its discriminant is $\Delta = 64$ according to

theorem 1.8 it is a non-singular curve. So we have a non-singular curve clearly of degree three and by genus-degree formula[3] we have that its genus is 1. And obviously if we set $Z = 0$ in the homogenized expression of the curve $Y^2Z - 9YZ^2 = X^3 - 27Z^3$ we get that the base point is $O = [0 : 1 : 0]$.

In case that we have that $charK = 3$ we have that the cubic $x^3 + y^3 + z^3 = 0$ would be singular. Hence, it wouldn't define an elliptic curve.

1.2 The Group Law

As an elliptic curve E over a field K is a plane non-singular curve, for every point $P \in E(\overline{K})$ it verifies that at least one of the partial derivatives is nonzero and so we can define a tangent line at every point of the curve. The tangent line L to E at a point $[x_0 : y_0 : z_0]$ is expressed by

$$L \ : \ X\left[\frac{\partial F}{\partial X}\right]_{(x_0,y_0,z_0)} + Y\left[\frac{\partial F}{\partial Y}\right]_{(x_0,y_0,z_0)} + Z\left[\frac{\partial F}{\partial Z}\right]_{(x_0,y_0,z_0)} = 0 \tag{1.3}$$

Where F denotes the equation that describes the elliptic curve E.

$$F(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$$

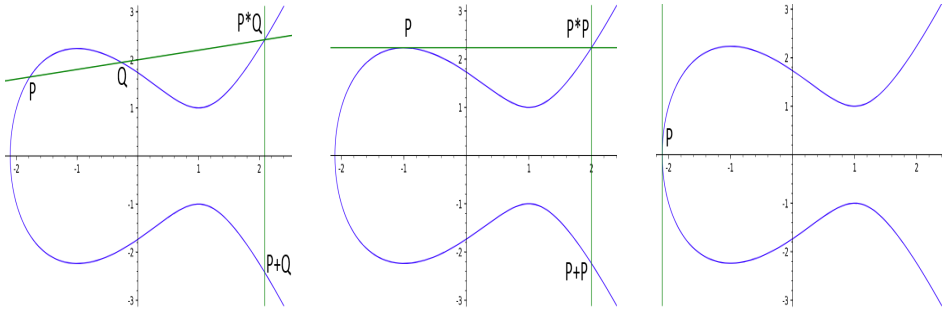
Given a line L it intersects with E at exactly three points since it is of degree three (it is a special case of Bezout's theorem). If L is tangent to E then the intersection points will be distinct. Given an elliptic curve E considering the set of all the points of the elliptic curve using the previous properties a composition law for this set can be worked out.
Starting with two points of the elliptic curve $P, Q \in E$ draw a line through them and get a third point of intersection of the line with the curve denoted by $P * Q$. When P and Q are the same point draw a tangent line at P and obtain a line that intersects the curve twice at the point P and meets the curve once again at a third intersection point. Even thought it might seem like it at first, the previous operation doesn't give a group structure for the set of the points of the elliptic curve E. Making small changes we do get to define the rule for the group law as follows, where we denote the operation by $+$:

Definition 1.14 (Composition Law)**.** Given $P, Q \in E$ and let L be the line through P and Q and $P * Q$ as the third point of intersection of E with L, in case that P and Q are the same L will be the tangent line to E at P . Let L' be the line through $P * Q$ and O which intersects with the cubic at a third point $P + Q$, which is the addition of P to Q. So, by definition $P + Q = O * (P * Q)$.

And the set of elliptic curves is a commutative group with the base point O as the neutral element and the composition law described above.

Remark 1.15. The fact that an elliptic curve is non-singular is important for the definition of the group law, since it means that there is a unique tangent line at every point. So we see that the given definition of addition is well-defined.

[3]The genus-degree formula relates the degree of a non-singular curve to its genus



(a) $P \neq Q$ (b) P = Q (c) $P = Q,\ 2P = O$

Figure 1.3: Singular curves

In the figure 1.3 we can visualize the different situations one might encounter when trying to add two points belonging to an elliptic curve. The first two situations (1.3a and 1.3b) have been precisely described in definition 1.14. As for 1.3c, when L is a tangent line at P that meets E again at O, then the third intersection point of L' through $P * P = O$ and O is going to be O, so clearly $2P := P + P = O$.

Proposition 1.16. *The composition law makes $E(\bar{K})$ into an abelian group with identity element O, i.e. verifies the following properties*

(a) If a line intersects E at three points (not necessarily distinct) P, Q, R, then

$$(P + Q) + R = O$$

(b) $P + O = P$ for all $P \in E$

(c) $P + Q = Q + P$ for all $P, Q \in E$

(d) Let $P \in E$. There is a point of E, denoted by $-P$ such that

$$P + (-P) = O$$

(e) Let $P, Q, R \in E$. Then

$$(P + Q) + R = P + (Q + R)$$

Moreover,

(f) Suppose E defined over K and let K'/K be a field extension. Then

$$E(K') = \{(x, y) \in K' \times K : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}$$

is a subgroup of $E(K')$

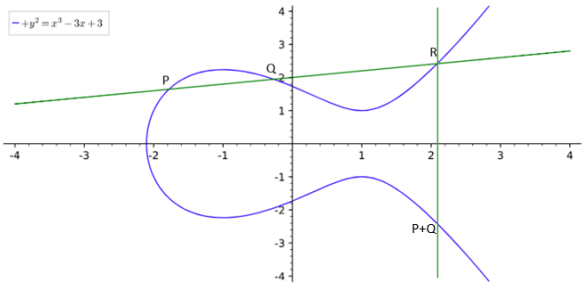


Figure 1.4: $(P+Q)+R=O$

Proof. (a) Note that in the figure 1.4 the tangent line to E at O intersects E at three points.

and it can be visualized that $(P+Q)+R=O$. It is clear that $(P+Q)*R=O$ and so $(P+Q)+R=O$.

(b) Using the definition of the composition law taking $Q=O$ the line through P and O intersects E in a third point R. And L' goes through R and O and $P+O$, so $P+O=O$.

(c) The construction of the composition law in 1.14 is symmetric in P and Q.

(d) Let P,Q,R are the intersection of a line L and E, and suppose $Q=O$. Using (a) it verifies that

$$O=(P+O)+R=P+R$$

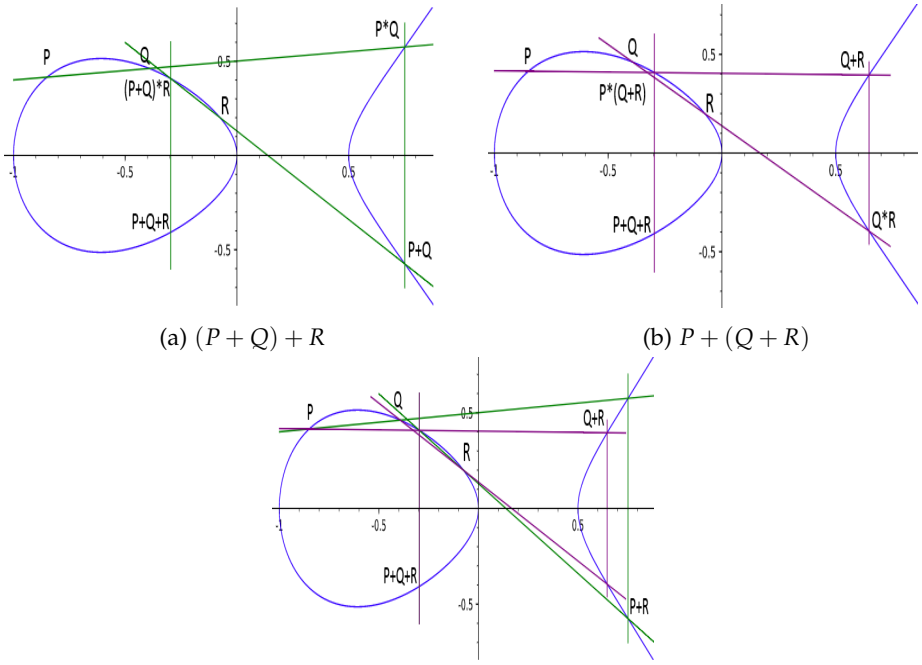
(e) The associative property can be verified using the explicit formulas case by case, which is rather technical. Instead, taking advantage of the geometrical definition of the addition, we have been able to do a rather visual proof in the figure 1.5. In the proof we have reproduced the addition of $(P+Q)+R$ on 1.5a, and the addition of $P+(Q+R)$ in 1.5b using the definition 1.14 . Then in order to be able to compare the two results we have 1.5c, where clearly we can see how $(P+Q)+R=P+(Q+R)$

(f) Suppose P and Q have coordinates in K', then the line L that goes through both of them has coefficients in K'. Since E is defined over K, then the third intersection point of E and L is expressed by a rational combination of the coordinates of coefficients of the curve and the line, so is in K'.

□

Remark 1.17. Given $P\in E$ and $n\in\mathbb{Z}$, then

$$nP=P+\overset{n}{\cdots}+P,\quad -nP=(-P)+\overset{n}{\cdots}+(-P),\quad 0P=O$$



(a) $(P+Q)+R$

(b) $P+(Q+R)$

(c) $(P+Q)+R = P+(Q+R)$

Figure 1.5: Associative property

Proposition 1.18 (Group Law Algorithm). *Let E be an elliptic curve given by Weierstrass general equation. Let $P_1 + P_2 = P_3$ with $P_i \in E$, $i = 1, 2, 3$*

(a) Let $P_0 = (x_0, y_0)$. Then $-P_0 = (x_0, -y_0 - a_1x_0 - a_3)$.

(b) If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$, then $P_1 + P_2 = O$.

We define $y = \lambda x + v$ line through P_1 and P_2, or tangent if $P_1 = P_2$, where

- *If $x_1 \neq x_2$, $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ and $v = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$*
- *If $x_1 = x_2$, $\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$ and $v = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$*

(c) $P_3 = P_1 + P_2$ has coordinates

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$$
$$y_3 = (-\lambda + a_1)x_3 - v - a_3$$

(c) Moreover, we have the duplication formula for $P = (x, y) \in E$

$$x([2]P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}$$

where b_i, $i = 2, 4, 6, 8$ have been introduced in the previous section.

The explicit formulas for the group operation on E can be easily found though step-by-step process of the composition law, described previously. It is a pretty technical calculus, so we have preferred to move forward. To those who would like to have a glance at details of the process, can refer to [6], [2], [7].

1.3 Endomorphisms

Let K a field and E an elliptic curve defined over K. In this chapter the object of interest is going to be a map from one elliptic curve to itself. From now on when referring to an endomorphism it will mean the following

Definition 1.19. Given an elliptic curve E/K an *endomorphism* is a map

$$\begin{aligned} \alpha \ : \ E &\longrightarrow E \\ (x,y) &\longmapsto (R_1(x,y), R_2(x,y)) \end{aligned}$$

that preserves the base point, i.e. $\alpha(O) = O$ and with $R_1(x,y), R_2(x,y)$ being quotients of polynomials.
We will say that α is defined over an extension K' of K if R_1, R_2 are quotients of polynomials with coefficients in $K'[X,Y]$.

Example 1.20. Given $n \in \mathbb{Z}$ we define *the multiplication-by-n* endomorphism

$$\begin{aligned} [n] \ : \ E &\longrightarrow E \\ P &\longmapsto P + \overset{n}{\cdots} + P \end{aligned}$$

When $n < 0$, $[n](P) = [-m](-P)$, and for $n = 0$, $[0](P) = O$. By induction it is easy to see that $[n]$ is a morphism , and it is clear that O is sent to O therefore it is an endomorphism.

Remark 1.21. Having defined the multiplication-by-n, we can talk about the subgroup of E of n-torsion points defined $E[n] := \{P \in E \ : \ nP = O\}$.

Proposition 1.22. *Let E be an elliptic curve over a field L and let n be a positive integer. If $charK \nmid n$ or it is 0, then*

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

If $charK = p$ and $p|n$, we can rewrite $p = p^r n'$, $r \in \mathbb{Z}$ in a way that $p \nmid n'$ and then

$$E[n] \cong \mathbb{Z}/n'\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z} \quad or \quad E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}$$

Proof. We will talk about it in the next section. Readers interested in a detailed proof can see [8], Chapter 3, theorem 3.2 . □

Before we continue with the theory there is another important example of an endomorphism.

Example 1.23. A special endomorphism that needs tot be mentioned is the Frobenius endomorphism. Let $K = \mathbb{F}_q$, a finite field of q elements where q is a power of a primer number p. The *Frobenius endomorphism* is defined as following

$$\begin{aligned} \phi_q : E(\overline{\mathbb{F}}_q) &\longrightarrow E(\overline{\mathbb{F}}_q) \\ (x,y) &\longmapsto (x^q, y^q) \\ O &\longmapsto O \end{aligned}$$

which is an extension of the Frobenius endomorphism we find over $\overline{\mathbb{F}_q}$

$$\begin{aligned} \overline{\mathbb{F}}_q &\longrightarrow \overline{\mathbb{F}}_q \\ x &\longmapsto x^q. \end{aligned}$$

Recall that the Frobenius isomorphisms fixes the field $\mathbb{F}_q$, it is easy to see that ϕ_q sends points of $E(\overline{\mathbb{F}_q})$ to points of $E(\overline{\mathbb{F}_p})$, assuming E defined over $\mathbb{F}_q$.

Having seen the example, we now move on to introduce some theory in order to define a degree of a morphism.

If we suppose that $charK \neq 2$, we have seen that the general Weierstrass equation of an elliptic curve can be transformed into $y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$, that clearly can be transformed into $y^2 = x^3 + ax^2 + bx + c$. And so in $R_1(x,y)$ and $R_2(x,y)$ we can replace any even power of y by a polynomial in x and any odd power of y by y times a polynomial in x and obtain that for $i = 1, 2$

$$R_i(x,y) = \frac{p_{1i}(x) + p_{2i}(x)y}{p_{3i}(x) + p_{4i}(x)y}$$

Moreover multiplying the numerator and denominator by $p_{3i} - p_{4i}y$ and then replacing y^2 by $4x^3 + b_2x^2 + 2b_4x + b_6$

$$R_i(x,y) = \frac{q_{1i}(x) + q_{2i}(x)y}{q_{3i}}.$$

As α is and homomorphism we get that $\alpha(-(x,y)) = \alpha((x,-y)) = -\alpha(x,y)$ and so $R_i(x,y) = R_i(x,-y)$ which brings us to the fact that $q_{21} = 0$ and $q_{12} = 0$ and so we can assume that

$$\begin{aligned} &\alpha(x,y) = (r_1(x), r_2(x)y), \quad r_1 = \frac{p(x)}{q(x)} \\ &\alpha(0,y) = O, \quad \forall\, y \end{aligned}$$

where $p(x)$ and $q(x)$ have no common factors.

Definition 1.24. The *degree* of α is $\max\{\deg(p(x)), \deg(q(x))\}$.

Remark 1.25.

- For $\alpha = 0$ we have that $\deg \alpha = 0$.
- For two endomorphisms $\alpha,\ \beta$ and two integers a, b we have that

$$\deg(a\alpha + b\beta) = a^2 \deg \alpha + b^2 \deg \beta + ab(\deg(\alpha + \beta) - \deg \alpha - \deg \beta)$$

Definition 1.26. Given $\alpha \neq 0$ we say that it is *separable* if $r_1'(x)$ is not identically zero.

Example 1.27. In case of the Frobenius endomorphism we have that $\deg \phi_q = q$, but as $\phi_q(x,y) = (x^q, y^q) = (r_1(x), r_2(x)y)$ then we have that $r_1'(x) = q(x)^{q-1} = 0$ since $charK = p$ and q is a power of p, so it is not separable. And clearly $\deg(\phi_q) = q$ since $r_1(x) = x^q$.

Remark 1.28. From now on we will no longer suppose that $charK \neq 2$.

Proposition 1.29. *Let $\alpha \neq 0$ an endomorphism of an elliptic curve E over K.*
If α is separable the $\deg \alpha = \#\operatorname{Ker} \alpha$.
If α is not separable the $\deg \alpha > \#\operatorname{Ker} \alpha$.

Proof. See [8]. Chapter 2. Proposition 2.21 . □

Remark 1.30. $\operatorname{Ker} \alpha = \alpha^{-1}(O)$.

Since the elliptic curves form an abelian group then also the endomorphisms between them form groups. And using composition as multiplication for the maps, one gets

Definition 1.31. The ring $End(E) = \{\alpha \mid \alpha : E \longrightarrow E \text{ endomorphism } \}$ is called *endomorphism ring of E*. The sum of two endomorphisms $\alpha, \beta : E \longrightarrow E$ is defined by

$$(\alpha + \beta)(P) = \alpha(P) + \beta(P),\ P \in E$$

The multiplication of two endomorphisms $\alpha, \beta : E \longrightarrow E$ is the composition defined by

$$(\alpha\beta)(P) = \alpha(\beta(P)),\ P \in E$$

And the invertible elements of $End(E)$ form a group.

Definition 1.32. The invertible elements of $End(E)$ form the *automorphism group* of E, denoted by $Aut(E)$.

Remark 1.33. When E is defined over a field K, then the previous can be restricted to the endomorphisms defined over K and denoted by $End_k(E),\ Aut_K(E)$

In the direction to see the ring endomorphism structure, we introduce some new concepts.

Definition 1.34. A finite field extension K of $\mathbb{Q}$ is called *algebraic number field* or *number field*.

Example 1.35.
- The most basic example is $\mathbb{Q}$.
- The quadratic field $K = \mathbb{Q}(\sqrt{d})$, for any square-free integer d.

Definition 1.36. An element $a \in K$ is called *integral* if it satisfies a monic equation

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0,\ a_i \in \mathbb{Z}\ \ 1 \leqslant i \leqslant n$$

Definition 1.37. The *ring of integers* of a number field K is the ring containing all integral elements in K. This ring is denoted by $\mathcal{O}_K$.

Example 1.38.
- We have mentioned that $\mathbb{Q}$ is the most basic example of a number field, and so clearly its ring of integers is $\mathbb{Z}$.
- In case of a quadratic field $K = \mathbb{Q}(\sqrt{d})$, we have that it is a ring of quadratic integers

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} + \sqrt{d}\mathbb{Z} & \text{if } d \equiv 2,3 \mod 4 \\ \mathbb{Z} + \frac{1+\sqrt{d}}{2}\,\mathbb{Z} & \text{if } d \equiv 1 \mod 4 \end{cases}$$

Remark 1.39. $\mathbb{Z}$ is always a subring of $\mathcal{O}_K$ since any integer number is an integral element of K.

Definition 1.40. Given K a number field, a subring R of K is called an *order* if it is finitely generated as a $\mathbb{Z}$-module and its field of fractions is K.

Example 1.41. Let K an imaginary quadratic field and $\mathcal{O}$ its ring of integers. Then $\mathbb{Z} + f\mathcal{O}$ with $a \in \mathbb{Z}$ is an order of K.

Remark 1.42. The ring of integers $\mathcal{O}_K$ of a number field K is the unique maximal order of K.

Proposition 1.43. *Suppose that $charK = 0$, the endomorphism ring of an elliptic curve E over K is either $\mathbb{Z}$ or an order in an imaginary quadratic field.*

Proof. We will talk about this proof in the next section.
The readers who would like to see a detailed proof can find it in [6], Chapter III, Corollary 9.4 . □

Remark 1.44. In fact we have that in case that $charK = 0$, and we have an elliptic curve E defined over K then the map

$$[\,] \;:\; \mathbb{Z} \longrightarrow End(E)$$

usually verifies that $End(E) \cong \mathbb{Z}$. When $End(E)$ is strictly larger than $\mathbb{Z}$ we then say that E has complex multiplication.
On the other hand, when K is a finite field, the $End(E)$ is always larger than $\mathbb{Z}$.

And so we can now define when an elliptic curve has complex multiplication.

Definition 1.45. Suppose $chark = 0$.We sat that an elliptic curve E over K has *complex multiplication* when it verifies that its endomorphism ring $End(E)$ is strictly larger than $\mathbb{Z}$.

Remark 1.46. As we have seen before, if E has complex multiplication, then $End(E)$ is an order in an imaginary quadratic field L. In this case we say that E/K has complex multiplication over L.

Example 1.47. Getting back to $x^3+y^3+z^3=0$, we would like to see what is its endomorphism ring.
If ξ is the third root of unity and $E: zy^2 = x^3 - 432z^3$ We take the map

$$\begin{array}{rccc} \alpha: & E(\mathbb{Q}(\sqrt{-3})) & \longrightarrow & E(\mathbb{Q}(\sqrt{-3})) \\ & [x:y:z] & \longmapsto & [x:\xi y:\xi z]. \end{array}$$

First of all notice that $\alpha(O) = \alpha(0,1,0) = [0:\xi:0]$, and since in $\mathbb{P}^2$ we have that $[0:\xi:0]$ and $[0:1:0]$ are the same we have that $alpha(O) = O$.
Clearly, if $[x:y:z]$ verifies E, then as $\alpha(x,y,z) = [x:\xi y:\xi z]$ we have that $\xi z(\xi y)^2 = x^3 - 432\xi^3$ is clearly $zy^2 = x^3 - 432z^3$ since the third root of unity verifies $\xi^3 = 1$. Hence $\alpha(x,y,z) \in E(\mathbb{Q})$.
So we have that α belongs to the endomorphism ring of E. We now would like to see its order in $End(E)$.

$$\begin{array}{ccccccccc} E(\mathbb{F}_p) & \xrightarrow{\alpha} & E(\mathbb{F}_p) & \xrightarrow{\alpha} & E(\mathbb{F}_p) & \xrightarrow{\alpha} & E(\mathbb{F}_p) \\ [x:y:z] & \longmapsto & [x:\xi y:\xi z] & \longmapsto & [x:\xi^2 y:\xi^2 z] & \longmapsto & [x:y:z] \end{array}$$

And so clearly we have that α has order three in $End(E)$ and it is not a multiplication-by-n endomorphism.
We now that in this case the endomorphism ring is an order in an imaginary quadratic field over $\mathbb{Q}$ by Proposition 1.43. And in fact the imaginary quadratic field is $\mathbb{Q}(\sqrt{-3}) = Q(\alpha)$. Since $-3 \equiv 1 \mod 4$ as we have seen in the example 1.38 the ring of integers will be $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. In fact, we have that $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] \simeq \mathbb{Z}[\alpha] \subseteq End(E) \subset \mathbb{Q}(\alpha) \simeq \mathbb{Q}(\sqrt{-3})$ and as a matter of fact the ring of integers is its maximal order so we have $End(E) = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$.
In conclusion, $y^2 = x^3 - 432$ has complex multiplication, and so does $x^3+y^3+z^3=0$.

In the sections to come we will see more on complex multiplication.

1.4 Complex Elliptic Curves

In this section we will present two important results regarding the structure of the n-torsion points as well as the structure of the endomorphism ring of a given elliptic curve $E/\mathbb{C}$.

Definition 1.48. We define *lattice* Λ in $\mathbb{C}$ as a subgroup of $\mathbb{C}$ containing an $\mathbb{R}$-basis $\{\omega_1, \omega_2\}$ for $\mathbb{C}$. We can write

$$\Lambda = \{n_1\omega_1 + \mathfrak{n}_2\omega_2 \ : \ n_1, n_2 \in \mathbb{Z}\}$$

Having defined a lattice, in fact what we are interested in is the study of meromorphic functions on $\mathbb{C}/\Lambda$.

Remark 1.49. Given $\Lambda \subset \mathbb{C}$ a lattice then $\mathbb{C}/\Lambda$ with its natural addition is a group.

Definition 1.50. Given $\Lambda \subset \mathbb{C}$ a lattice. We define the *Weierstrass $\wp$- function* to be

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$

Remark 1.51. The Weierstrass $\wp$-function relative to a lattice Λ is absolutely convergent for all $z \in \mathbb{C}/\Lambda$, therefore we can derive term by term and have that

$$\wp'(z;\Lambda) = -2 \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \frac{1}{(z-\omega)^3}$$

Proposition 1.52. *Let $\Lambda \subset \mathbb{C}$ be a lattice and $g_2 = g_2(\Lambda)$, $g_3 = g_3(\Lambda)$ quantities associated to the lattice.*
Then we have that

$$f(x) = 4x^3 - g_2 x - g_3$$

has distinct roots, so its discriminant $\Delta(\Lambda) = g_2^3 - 27g_3^2$ is nonzero.
Moreover, let $E/\mathbb{C}$ be an elliptic curve

$$E \ : \ y^2 = 4x^3 - g_2 x - g_3$$

since we have that its discriminant is nonzero. Then the map

$$\begin{aligned} \phi \ : \ \mathbb{C}/\Lambda &\longrightarrow E(\mathbb{C}) \subset \mathbb{P}(\mathbb{C}) \\ x &\longmapsto [\wp(z), \wp'(z), 1] \end{aligned}$$

is an isomorphism that is also a group homomorphism.

Proof. See [6], Chapter VI, Proposition 3.6 . □

As for the quantities associated to the lattice Λ in the previous proposition, they come from relation established between the Weierstrass $\wp$-function and its derivative.

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3, \ \ g_2 = 60G_4(\Lambda) \text{ and } g_3 = 140G_6(\Lambda)$$

where

$$G_{2k}(\Lambda) = \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \omega^{-2k} \text{ with } k = 1, 3$$

Remark 1.53. And so the Proposition 1.52 states that given a lattice $\Lambda \in \mathbb{C}$ we can associate an elliptic curve to it that would be equivalent to $\mathbb{C}/\Lambda$.
Moreover given $E_1/\mathbb{C}$ associated to a lattice Λ_1 and $E_2/\mathbb{C}$ associated to a lattice Λ_2. Then the two elliptic curves E_1 and E_2 are isomorphic over $\mathbb{C}$ if and only if there exists $\alpha \in \mathbb{C}^\times$ such that $\Lambda_1 = \alpha\Lambda_2$. When such α exists we say that the lattices are *homothetic*. In this framework we shall state uniqueness up to homothety

In fact we can see the previous result in the other way around.

Theorem 1.54. Uniformization Theorem *Let A, B be complex numbers satisfying that $A^3 - 27B^2$ is nonzero. Then there exists a unique lattice $\Lambda \in \mathbb{C}$ such that*

$$g_2(\Lambda) = A \text{ and } g_3(\Lambda) = B$$

Proof. See [5], Chapter I, Corollary 4.3 . □

Corollary 1.55. *Given $E/\mathbb{C}$ an elliptic curve. Then there exists a lattice $\Lambda \subset \mathbb{C}$, unique up to homothety, and a group isomorphism*

$$\begin{aligned} \phi \ : \ {}^{\mathbb{C}}/_{\Lambda} &\longrightarrow E(\mathbb{C}) \subset \mathbb{P}(\mathbb{C}) \\ x &\longmapsto [\wp(z), \wp'(z), 1] \end{aligned}$$

Proof. The existence is due to Proposition 1.52 and the theorem 1.54, as for the uniqueness it is consequence of the remark 1.53. □

Now we want to use the theory applied to see the structure of the n-torsion points as well as of the endomorphism ring of an elliptic curve $E/\mathbb{C}$.

Remark 1.56. If we have an elliptic curve $E/\mathbb{C}$ with a lattice given by the following expression $\Lambda = \{n_1\omega_1 + n_2\omega_2 \ : \ n_1, n_2 \in \mathbb{Z}\} \subset \mathbb{C}$, then n-torsion points are of the form

$$\left({}^{\mathbb{C}}/_{\Lambda}\right)[n] = \left\{ \frac{n_1}{n}\omega_1 + \frac{n_1}{n}\omega_2 \ : \ n_1, n_2 \in {}^{\mathbb{Z}}/_{n\mathbb{Z}} \right\}$$

Proposition 1.57. *Given an elliptic curve $E/\mathbb{C}$ and $n \geqslant 1$ an integer. There is an isomorphism*

$$E[n] \cong {}^{\mathbb{Z}}/_{n\mathbb{Z}} \times {}^{\mathbb{Z}}/_{n\mathbb{Z}}$$

Proof. We have already seen that $E(\mathbb{C})$ is isomorphic to ${}^{\mathbb{C}}/_{\Lambda}$ for some lattice $\Lambda \subset \mathbb{C}$, therefore keeping in mind the remark 1.56

$$\begin{aligned} E[n] \cong \left({}^{\mathbb{C}}/_{\Lambda}\right)[n] &\cong \left(\tfrac{1}{n}\Lambda\right)/_{\Lambda} \\ &\cong {}^{\mathbb{Z}}/_{n\mathbb{Z}} \times {}^{\mathbb{Z}}/_{n\mathbb{Z}} \end{aligned}$$

just as we wanted to prove. □

Now we move on to the endomorphism rings with this first remark and some necessary information before we can prove its structure.

Remark 1.58. As for the endomorphism, given $E/\mathbb{C}$ and Λ a lattice such that $E \cong {}^{\mathbb{C}}/_{\Lambda}$. And suppose that $\phi \in End(E)$, then there exists $c \in \mathbb{C}$ such that the induced homomorphism of ϕ on ${}^{\mathbb{C}}/_{\Lambda}$ is given by

$$\begin{aligned} {}^{\mathbb{C}}/_{\Lambda} &\longrightarrow {}^{\mathbb{C}}/_{\Lambda} \\ z + \Lambda &\longmapsto cz + \Lambda \end{aligned}$$

which is well-defined when $c\Lambda \subset \Lambda$ and doesn't depend on the choice of Λ.
The previous relation allows us to identify $End(E)$ with a certain subring of $\mathbb{C}$. And so if have an elliptic curve $E/\mathbb{C}$ corresponding to a lattice Λ ,unique up to homothety, such that $E(\mathbb{C}) \cong {}^{\mathbb{C}}/_{\Lambda}$, then

$$End(E) \cong \{\alpha \in \mathbb{C} \ : \ \alpha\Lambda \subset \Lambda\} =: R(\Lambda)$$

Proposition 1.59. *Given an elliptic curve E defined over $\mathbb{C}$ and its associated lattice $\Lambda = \{n_1\omega_1 + n_2\omega_2 : n_1, n_2 \in \mathbb{Z}\}$. Then the endomorphism of E is either $\mathbb{Z}$ or an order in a quadratic imaginary extension $\mathbb{Q}(\omega_2/\omega_1)$.*

Proof. Denote $\tau = \omega_2/\omega_1$.
Be aware that

$$End(E) \cong \mathcal{R} = \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}$$

Now if we take $1/\omega_1$ we know that $\frac{1}{\omega_1}\Lambda$ is homomothetic to Λ so we can replace it by $\mathbb{Z} + \tau\mathbb{Z}$ since $\mathcal{R}$ doesn't depend on Λ. And so for any $\alpha \in \mathcal{R}$ there are integers a, b, c, d such that

$$\alpha = a + b\tau \text{ and } \alpha\tau = c + d\tau$$

Eliminating τ from the previous equation we get the following equation

$$\alpha^2 - (a + d)\alpha + ad - bc = 0$$

And so every element $\alpha \in \mathcal{R}$ is a root of the polynomial $x^2 - (a + d)x + ad - bc = 0$ is integral therefore R is an integral extension of $\mathbb{Z}$.
Suppose that $\mathcal{R} \neq \mathbb{Z}$ and that now $\alpha \in \mathcal{R} \setminus \mathbb{Z}$, so necessarily $b \neq 0$ in the expressions

$$\alpha = a + b\tau \text{ and } \alpha\tau = c + d\tau$$

Note that $(\alpha - d)\tau - c = 0$ which is equivalent to $(\alpha - d)\omega_2 - \omega_1 c = 0$ and by definition of lattice ω_1 and ω_2 are $\mathbb{R}$-linearly independent, and since $\alpha \neq d \in \mathbb{Z}$ then $\alpha - d \notin \mathbb{R}$. And since α is expressed in terms of $a, b\tau$ and a and b are integers $\tau \notin \mathbb{R}$. Now we eliminate α and get that

$$b\tau^2 + (a - d)\tau - c = 0$$

and so τ is a root of $p(x) = bx^2 + (a - d)x - c$ so an algebraic integer with $p(x)$ as a minimal polynomial over $\mathbb{Q}$ of degree two. So since $\tau \notin \mathbb{R}$ then $\mathbb{Q}(\tau)$ is an imaginary quadratic extension of $\mathbb{Q}$. Moreover, since $\mathcal{R} \subset \mathbb{Q}(\tau)$ and $\mathcal{R}$ is integral over $\mathbb{Z}$, then $\mathcal{R}$ is an order in $\mathbb{Q}(\tau)$.
So in conclusion, since $\mathcal{R}$ is isomorphic to $End(E)$ we have seen that it is either $\mathbb{Z}$ or an order in a quadratic imaginary field extension. □

Remark 1.60. Lefschetz principle states that the algebraic geometry over $\mathbb{C}$ is equivalent to the algebraic geometry over an arbitrary algebraic closed number field of characteristic 0 using category theory. Therefore, using Lefschetz principle the previous results on the structure of the endomorphisms and of the n-torsion points are immediate for an elliptic curve over a field K of characteristic 0. Moreover we can generalize it as well for any field K adding some more cases into the proofs which we will not get to since they are very extent and we have already had a look into it. In fact we have already spoken about structure of endomorphism ring in the Proposition 1.43, and about the structure of the n-torsion points in the Proposition 1.22, which can be considered proved now when $charK = 0$.

We will now see a little more about complex multiplication on complex elliptic curves. We will first get familiar with the concept of a class group over an algebraic number field. The idea behind a class group is to measure how far is the ring of integers $\mathcal{O}$ of being a principal ideal domain. Before we move on to the definition we need to define a fractional ideal.

Definition 1.61. *A fractional ideal of K is a finitely generated $\mathcal{O}$-submodule $\mathfrak{a} \neq 0$ of K. The fractional ideals form an abelian group J_K ideal group.*

Definition 1.62. *We define the ideal class group or class group of K to be the quotient group*

$$Cl_K = J_K \,/ P_K$$

where P_K is the subgroup of J_K of fractional principal ideals $(a) = a\mathcal{O}$, $a \in K^\times$

As we have mentioned, the class group measures how far the ring of integers is $\mathcal{O}$ from being a principal ideal domain. More precisely it is its order that gives us this information, which is called *class number*.

Remark 1.63. The class number is finite. If $\mathcal{O}$ has class number 1, then it is a principal ideal domain.

Proposition 1.64. *Given an imaginary quadratic field $K/\mathbb{Q}$, $\mathcal{O}$ its ring of integers and $Cl(\mathcal{O})$ the ideal class group of $\mathcal{O}$, there is one-to-one correspondence between ideal classes in $Cl(\mathcal{O})$ and isomorphism classes of elliptic curves $E/\mathbb{C}$ with $End(E) \cong \mathcal{O}$*

Proof. First of all we fix an embedding $K \subset \mathbb{C}$, then each ideal $\Lambda \in \mathcal{O}$ is a lattice $\Lambda \in \mathbb{C}$, so we can consider the elliptic curve $\mathbb{C}\,/\Lambda$ and have that

$$End(\mathbb{C}\,/\Lambda) \cong \{\Lambda \in \mathbb{C} \ : \ \alpha\Lambda \subset \Lambda\} = \mathcal{O}$$

And by the Remark 1.53 we have that the elliptic curve $\mathbb{C}\,/\Lambda$ depends only on the ideal class $\{\Lambda\} \in Cl(\mathcal{O})$, up to isomorphism.
On the other hand, if $E/\mathbb{C}$ satisfies that $End(E) \cong \mathcal{O}$ by Corollary 1.55 $E(\mathbb{C}) \cong \mathbb{C}\,/\Lambda$ for a unique ideal $\{\Lambda\} \in Cl(\mathcal{O})$. □

Corollary 1.65. *There are only finitely many isomorphism classes of elliptic curves $E/\mathbb{C}$ with $End(E) \cong \mathcal{O}$.*

Proof. Since we now that the ideal class group $Cl(\mathcal{O})$ is of finite order, then by the previous proposition, there are indeed only finitely many isomorphism classes of elliptic curves $E/\mathbb{C}$ with $End(E) \cong \mathcal{O}$. □

Example 1.66. The previous remark is true when we have $\Lambda = \mathcal{O}$. Then we will have that $\mathbb{C}\,/\Lambda$ is isomorphic to an elliptic curve $E/\mathbb{C}$ such that $End(E) \cong \mathcal{O}$.
In fact, there are exactly nine imaginary quadratic fields with class number one, which are $\mathbb{Q}(\sqrt{-d})$ with $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$

Example 1.67. There are as well example in case when, $End(E)$ is an arbitrary order in K, instead of the full ring of integers. In this case, $End(E) \cong \mathbb{Z} + f\mathcal{O}$, for some integer f, where f is called the *conductor* of the order and is the index of the order in $\mathcal{O}$

1.5 Elliptic curves over Finite Fields

In this section , suppose $K = \mathbb{F}_q$ a finite field with q elements and $charK = p$ ($q = p^r$ for some integer r and a prime p). Let E be an elliptic curve in Weierstrass form defined over $\mathbb{F}_q$.

Definition 1.68. If the coordinates x and y of the solution to the elliptic curve E lie in $\mathbb{F}_q$ it is called *rational point*.

The theory seen so far was for any field K and so it still verifies for a finite field $\mathbb{F}_q$.

Remark 1.69. There are a finitely many possibilities for x and y for the solutions of E, and so it is clear that $E(\mathbb{F}_q)$ is a finite group.

Theorem 1.70. *Given E an elliptic curve over $\mathbb{F}_q$ then*

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z} \text{ or } E(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$$

for some integer $n \geqslant 1$, or for some integers $n_1, n_2 \geqslant 1$ with n_1 dividing n_2.

Proof. In case $\#E(\mathbb{F}_q) > 1$ from the finite abelian group structure theorem we have that given $r \in \mathbb{N}$

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}, \;\; n_i | n_{i+1} \text{ for } i \geqslant 1$$

If we have $E[n_1] = \{P \in E \; : \; n_1 P = O\} = \text{Ker}[n_1]$, and so using Proposition 1.29 and the fact[4] that $deg([n_1]) = n_1^2$ we have $\#\text{Ker}[n_1] \leqslant \deg([n_1]) = n_1^2$ so $\#E[n_1] \leqslant n_1^2$. Moreover since

$$\mathbb{Z}/n_1\mathbb{Z} \leqslant \mathbb{Z}/n_i\mathbb{Z}, \;\; 1 < i \leqslant r$$

we have that there will be at least n_1 n_1-torsion points in every $\mathbb{Z}/n_i\mathbb{Z}$, $1 < i \leqslant r$. Hence $E(\mathbb{F}_q)$ has at least n_1^r n_1-torsion points but since $\#E[n_1] \leqslant n_1^2$ then $r \leqslant 2$. In case that $r = 0$ then we set $n = 1$. □

We want to estimate the number of points in $\mathbb{F}_q$. We will start with some examples where we see how many solutions there are of an elliptic curve over a finite field.
As we have already mentioned, since we are looking for the solutions in a finite field $\mathbb{F}_q$, there are finitely many options for x and for y.
One approach to the problem can be substituting all the possibilities into our elliptic curve.

Example 1.71. For example, take

$$y^2 = x^3 + x + 1$$

[4] See [8]. Chapter 2

over $\mathbb{F}_5$. In order to count points on E, since x is in $\mathbb{F}_5$, we can substitute all the possible x in $x^3 + x + 1$ and see what results are a square in $\mathbb{F}_p$.

$\underline{x}$	$\underline{x^2 + x + 1}$	$\underline{y}$	*Points*
0	1	± 1	$(0,1), (0,4)$
1	3	$-$	$-$
2	1	± 1	$(2,1), (2,4)$
3	1	± 1	$(3,1), (3,4)$
4	4	± 2	$(4,2), (4,3)$
O		O	O

And so we see that $E(\mathbb{F}_5)$ has order 9.

Example 1.72. Now we can consider an elliptic curve E given by $y^2 + xy = x^3 + 1$ defined over $\mathbb{F}_2$. Using a similar method as before we have that

- If $x = 0$, then $y^2 = 1$, and so we have that $y = \pm 1$. Since $1 \equiv -1 \mod 2$, we have the point $(0,1)$ in $E(\mathbb{F}_2)$.
- If $x = 1$, then $y^2 + y = 0$ and the possibilities are $y = 0, 1$. We have the points $(1,0), (1,1)$ in $E(\mathbb{F}_2)$.

All in all, we find that

$$E(\mathbb{F}_2) = \{O, (0,1), (1,0), (1,1)\}$$

This is a cyclic group of order 4.
Now we move on to $E(\mathbb{F}_4)$. $\mathbb{F}_4$. As we now $\mathbb{F}_4$ is a finite field with 4 elements, so we can write it as $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ such that $\omega^3 = 1$. And using a similar method we have that

- If $x = 0$, then $y^2 = 1$ and $y = 1$. We get the point $(0,1)$.
- If $x = 1$, then $y^2 + y = 0$ and $y = 0, 1$. And the points will be $(1,0), (1,1)$.
- If $x = \omega$, then $y^2 + \omega y = 0$ and $y = 0, \omega$. The points are $(\omega, 0), (\omega, \omega)$.
- If $x = \omega^2$, then $y^2 + \omega^2 y = 0$ and $y = 0, \omega^2$. So the points are $(\omega^2, 0), (\omega^2, \omega^2)$.

We therefore get that its order is 8, with the following elements.

$$E(\mathbb{F}_4) = \{O, (0,1), (1,0), (1,1), (\omega, 0), (\omega, \omega), (\omega^2, 0), (\omega^2, \omega^2)\}$$

We have seen that counting the points isn't immediate or trivial. Luckily, we have that

Theorem 1.73. Hasse[3] *Let E an elliptic curve defined over a finite field $\mathbb{F}_q$. Then*

$$\left| \#E(\mathbb{F}_q) - q - 1 \right| \leqslant 2\sqrt{q}$$

Before we can prove it we would like to introduce some results.

[3] More general result for non-singular irreducible curves of genus g was conjectured by E. Artin in his thesis, and was proved by Hasse for elliptic curves, and by Weil for arbitrary g

Proposition 1.74. *Given E an elliptic curve defined over $\mathbb{F}_q$ and let r and s be non-zero integers. The endomorphism $r\phi_1 + s$ is separable if and only if $p \nmid s$.*

Proof. See [8]. Chapter 2. Proposition 2.29. □

Proof Theorem 1.73. First of all we want to suppose that $p \neq 2$ so we can apply the theory seen in the previous section but it does apply as well to $\mathbb{F}_q$ with $char\mathbb{F}_q = 2$. See that

$$\begin{aligned} E(\mathbb{F}_q) &= \{(x,y) \in E(\mathbb{F}_q) \ : \ \phi_q(x,y) = (x,y)\} \cup \{O\} \\ &= \{(x,y) \in E(\mathbb{F}_q) \ : \ (\phi_q - 1)(x,y) = \{O\} \\ &= \operatorname{Ker}(\phi_q - 1) \end{aligned}$$

By Proposition 1.74 since $p \nmid 1$ we conclude that by Proposition 1.29

$$\#E(\mathbb{F}_q) = \#\operatorname{Ker}(\phi_q - 1) = \deg(\phi_q - 1)$$

And in the example 1.27 we have seen that $\deg(\phi_q) = q$, since $[-1] = (x, -y)$ so $\deg([-1]) = 1$. By Proposition 1.25 we have that if $r, s \in \mathbb{Z}$ and $(q, s) = 1$

$$\begin{aligned} \deg(r\phi - s) &= r^2 \deg(\phi) + s^2 \deg([-1]) - rs(\deg(\phi_q - 1) + \deg \phi_q + \deg([-1])) \\ &= r^2 q + s^2 - rs(\#E(\mathbb{F}_p) + q + 1) \geqslant 0 \end{aligned}$$

Suppose $s \neq 0$ and divide by s^2

$$\frac{r}{s}^2 q + 1 - \frac{r}{s}(\#E(\mathbb{F}_p) + q + 1) \geqslant 0$$

to simplify the notation we denote $a = \#E(\mathbb{F}_p) + q + 1$ and suppose $x = \frac{r}{s}$

$$x^2 q + 1 - xa \geqslant 0$$

for all x real. So its discriminant $a^2 - 4q \leqslant 0$ therefore $|a| \leqslant 2\sqrt{q}$ just what we wanted to prove $|\#E(\mathbb{F}_p) + q + 1| \leqslant 2\sqrt{q}$. □

Now we will introduce some more results related to the amount of points of an elliptic curve over a finite field.

Theorem 1.75. *Given an elliptic curve E over $\mathbb{F}_q$ and let $\#(\mathbb{F}_q) = 1 + q - a$. Write*

$$X^2 - aX + q = (X - \alpha)(X - \beta), \ \ \alpha\beta = q, \ \ \alpha + \beta = a$$

We have that $\mathbb{F}_q \subset \mathbb{F}_{q^n}$, and then

$$\#E(\mathbb{F}_{q^n}) = 1 + q^n - (\alpha^n + \beta^n), \ \ \forall\, n \geqslant 1$$

Now before we can prove this result, we first need to see that $\alpha^n + \beta^n$ is an integer.

Lemma 1.76. *Let $s_n = \alpha^n + \beta^n$. Then we have $s_{n+1} = as_n - qs_{n-1}$ for all $n \geqslant 1$.*

Proof. First of all notice that $s_0 = 2$ and $s_1 = \alpha + \beta = a$. By definition we know that α and β are roots of $X^2 - aX + q$, and so we have that

$$\alpha^2 - a\alpha + q = 0$$
$$\beta^2 - a\beta + q = 0$$

Now multiplying the first equality by α^{n-1} and the second one by β^{n-1}, we get that

$$\alpha^{n+1} = a\alpha^n + q\alpha^{n-1} = 0$$
$$\beta^{n+1} = a\beta^n + q\beta^{n-1} = 0$$

and putting the last two equations together we obtain that $s_{n+1} = as_n - qs_{n-1}$ □

Remark 1.77. From the previous Lemma it follows that $\alpha^n + \beta^n$ is an integer.

We need one more result that we are going to use to prove the Theorem 1.75. First of all we have the following remark.

Remark 1.78. Given an elliptic curve E over K and an endomorphism $\alpha : E(\overline{K}) \longrightarrow E(\overline{K})$ we can associate a matrix representation to it. Clearly we have that $E(\overline{K}) \geqslant E[n]$, and so

$$\begin{array}{ccc} \alpha & : E(\overline{K}) & \longrightarrow E(\overline{K}) \\ & \vee\!/ & \vee\!/ \\ \alpha_n & : E[n] & \longrightarrow E[n] \end{array}$$

And we know that $P \in E[n]$ if and only if $nP = O$, and so $n(\alpha(P)) = \alpha(nP) = O$, and so we have that α_n is in fact a group homomorphism.
Furthermore we have seen in the Proposition 1.22 that $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. And if we take $T_1,\ T_2$ a basis for $E[n]$ and have that

$$\alpha_n(T_1) = aT_1 + cT_2, \qquad \alpha_n = bT_1 + dT_2$$

And then to α we associate the following matrix representation

$$\alpha_n = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Mat_{2\times 2}\left(\mathbb{Z}/n\mathbb{Z}\right)$$

Moreover,

$$det(\alpha_m) = \deg \alpha \mod n$$

Example 1.79. We can do the same in case of the Frobenius endomorphism that is defined over $E(\overline{\mathbb{F}_q})$ where $= p^r$ for some $r \in \mathbb{Z}$, but we should be aware that by Proposition 1.22 we need a $m \in \mathbb{Z}$ such that $p \nmid m$ in order to get that $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Its matrix representation will be the following

$$(\phi_q)_m = \begin{pmatrix} s & t \\ u & v \end{pmatrix} \in Mat_{2\times 2}\left(\mathbb{Z}/m\mathbb{Z}\right)$$

This matrix describes the action of ϕ_q on $E[m]$.

Theorem 1.80. *Given E an elliptic curve over $\mathbb{F}_q$. And given $a = q + 1 - \#E(\mathbb{F}_q) = q + 1 - deg(\phi_q - 1)$. Then*

$$\phi_q^2 - a\phi_q + q = 0$$

as endomorphisms of E. There is a unique integer k such that

$$\phi_q^2 - k\phi_q + q = 0$$

as endomorphisms and a is the only integer such that this relation holds for all $P \in E(\overline{\mathbb{F}}_p)$. Moreover, a is the unique integer satisfying

$$a = trace\left((\phi_q)_m\right) \mod m$$

for all m such that $(m, q) = 1$

Proof. For simplicity we will assume $charK \neq 2$.
First of all note that if ϕ_q is not the 0 endomorphism, then its kernel is finite by Proposition 1.29 .
And now we take $m \geqslant 1$ such that $(m, q) = 1$ work with the matrix associated to ϕ_q that we have seen in the example 1.79. And by Proposition 1.74 we have that $\phi_q - 1$ is separable, with induced matrix

$$(\phi_q)_m = \begin{pmatrix} s-1 & t \\ u & v-1 \end{pmatrix}$$

. Using the Proposition 1.29 and the remark 1.78 we have that

$$\#E(\mathbb{F}_q) = \#Ker(\phi_q - 1) = \deg(\phi_q - 1) \equiv (s-1)(v-1) - ut \mod m$$

By remark 1.78, $sv - tu = det((\phi_q)_m) \equiv q \mod m$ since $\deg \phi_q = q$.
And so we have that $\#Ker(\phi_q - 1) = q + 1 - a$, so

$$q + 1 - a \equiv (sv - tu) + 1 - (s + v) \mod m \equiv q + 1 - (s + v) \mod m$$

and in conclusion $(s + v) \equiv a \mod m$,ans so we have just proved that $a = trace\left((\phi_q)_m\right)$ mod m for all m such that $(m, q) = 1$.
By Cayley-Hamilton theorem we get that

$$\left((\phi_q)_m\right)^2 - a(\phi_q)_m + qI = 0 \text{ on } E[m]$$

where I is the 2×2 identity matrix . And since there are infinitely many choices for m, then kernel of $\phi_q^2 - a\phi_q + q$ is infinite, so the endomorphism is 0.
Suppose now that there is another integer $a_1 \neq a$ such that $\phi_q^2 - a_1\phi_q + q = 0$ as an endomorphism. And

$$(a - a_1)\phi_q = (\phi_q^2 - a\phi_q + q) - (\phi_q^2 - a_1\phi_q + q) = 0$$

So we have that $E[m] \subseteq \text{Ker}[a - a_1]$ for all m such that $p \nmid m$ and $a - a_1 \equiv 0 \mod m$. Hence $a = a_1$. And so we have proved the theorem. □

Remark 1.81. $X^2 - aX + q$ is often called the *characteristic polynomial of Frobenius*.

Now we move on to prove the Theorem 1.75.

Proof Theorem 1.75. As we have already mentioned by Lemma 1.76 we have that $\alpha^n+\beta^n$ is an integer for all $n \geqslant 0$.
Let

$$\begin{aligned} f(X) &= (X^n-\alpha^n)(X^n-\beta^n) = X^{2n}-(\alpha^n+\beta^n)X^n+(\alpha\beta)^n \\ &= X^{2n}-s_nX^n+q^n \in \mathbb{Z}[X] \end{aligned}$$

Clearly α and β are roots of $f(X)$, therefore $X^2-aX+q=(X-\alpha)(X-\beta)$ divides $f(X)$. And so there exists a polynomial $Q(X) \in \mathbb{Z}[X]$ such that $f(X)=Q(X)(X^2-aX+q)$. Since the polynomials are in $\mathbb{Z}[X]$, we can evaluate it in the endomorphism ϕ_q, and by Theorem 1.80

$$f(\phi_q) = Q(\phi_q)(\phi_q^2-a\phi_q+q)=0$$

as an endomorphism. Note that $\phi_q^n=\phi_{q^n}$, therefore

$$f(\phi_q)=\phi_q^n-(\alpha^n+\beta^n)\phi_q^n+q^n=\phi_{q^n}-(\alpha^n+\beta^n)\phi_{q^n}+q^n=0$$

By Theorem 1.80 there is only one $\alpha^n+\beta^n$ and it is determined by in the following way

$$\#E(\mathbb{F}_{q^n}) = q^n+1-(\alpha^n+\beta^n)$$

for all $n \geqslant 1$, which proves the theorem. □

As for the complex multiplication in elliptic curves over a finite field $\mathbb{F}_q$ it is important to mention the following remark.

Remark 1.82. Given E an elliptic curve over a finite field of characteristic p, if $\#E[p]=p$, then $End(E)$ is an order in an imaginary quadratic field.
Moreover, to know weather an elliptic curve verifies that $\#E[p]=p$ or not we have the following. If E is an elliptic curve defined over $\mathbb{Q}$ with good reduction at p, i.e. it is nonsingular modulo p. And we suppose that E has complex multiplication by an order in $\mathbb{Q}(\sqrt{-d})$. Then E has that $\#E[p]=p$ modulo p if $-d$ is a nonzero square $\mod p$. Such elliptic curves are called *ordinary*.

1.6 The curve $x^3+y^3+z^3=0$ and Gauss' Theorem

Theorem 1.83 (Gauss). *Let p be a prime and M_p the number of projective solutions to the equation*

$$x^3+y^3+z^3=0$$

with x,y,z in the field $\mathbb{F}_p$

- *If $p \not\equiv 1 \pmod 3$, then $M_p=p+1$.*
- *If $p \equiv 1 \pmod 3$, then there are integers A and B such that*

$$4p = A^2+27B^2$$

A and B are unique up to changing their signs, and if we fix a sign of A so that $A \equiv 1 \ (mod\ 3)$, *then*

$$M_p = p + 1 + A$$

Proof. First of all, we assume that $p \not\equiv 1 \ (mod\ 3)$. So we have that $p - 1 \not\equiv 0 \ (mod\ 3)$ and so 3 does not divide the order $p - 1$ of the cyclic group $\mathbb{F}_p$. Hence,

$$\begin{array}{ccc} \mathbb{F}_p & \longrightarrow & \mathbb{F}_p \\ x & \longmapsto & x^3 \end{array}$$

is an isomoprhism and so every element of $\mathbb{F}_p$ has a unique cube root.
We the have that the number of solutions of $x^3 + y^3 + z^3 = 0$ is equal to the number of solutions in the equation $x + y + z = 0$. Since $x + y + z = 0$ is the equation of a line in the projective plane, it has exactly $p + 1$ solutions over $\mathbb{F}_p$, since a finite projective plane has $p + 1$ points on each line. Indeed, for simplicity consider the line $y = ax + bz$. Either $z = 0$ and the line has the point $[1 : a : 0]$ or $z \neq 0$ and $y = ax + b$ has as many points as $x \in \mathbb{F}_p$. This is p points plus the "point at infinity" and $M_p = p + 1$.
As for when $p \equiv 1 \mod 3$, it is a rather long proof that using the same map and Galois theory as well as cubic residues gets to see that there are integers A and B such that $4p = A^2 + 27B^2$, which are uniquely determined up to their signs, and $M_p = p + 1 + A$.
For all the details see [7], Chapter 4.2, Theorem 4.2 . □

First of all we will see that Hasse's theorem verifies.
We denote M_p the number of solutions in the finite field $\mathbb{F}_p$.
First we start with the case when $p \not\equiv 1 \mod 3$ and $M_p = p + 1$ so clearly $|M_p - p - 1| \leqslant 2\sqrt{p}$.
When $p \equiv 1 \mod 3$ then there are integers A and B such that $4p = A^2 + 27B^2$ that implies that $A^2 \equiv 1 \mod 3$. So $A \equiv \pm 1 \mod 3$, and replacing when necessary $-A$ by A we can always have $A \equiv 1 \mod 3$. Besides since $B^2 > 0$, it follows that $A^2 = 4p + 27B^2 < 4p$ so $|A| \leqslant 2\sqrt{p}$ and we have that $M_p = p + 1 + A$. And so in fact the curve in the Gauss theorem verifies Hasse's theorem.

Moreover we would like to revise the results we have seen so far on the cubic $x^3 + y^3 + z^3 = 0$.

First of all we have seen that in fact it is an elliptic curve, with discriminant 64, that can be transformed into a Weierstrass form $E : y^2 = x^3 - 432$ over $\mathbb{Q}$ by using the map

$$\begin{array}{rccc} \theta : & \mathbb{P}_2 & \longrightarrow & \mathbb{P}_2 \\ & [X : Y : Z] & \longmapsto & [-12Z : -36(X - Y) : X + Y]. \end{array}$$

For characteristic 0 or $\geqslant 5$.

Furthermore, we have found an element of $End(E)$ of order three that is not a multiplication-by-n

$$\begin{array}{rccc} \alpha : & E(\mathbb{Q}) & \longrightarrow & E(\mathbb{Q}) \\ & [x : y : z] & \longmapsto & [x : \xi y : \xi z]. \end{array}$$

Therefore, we can conclude that the endomorphism ring of E is in fact $End(E) = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ and that the field of fractions of $End(E)$ is $\mathbb{Q}(\sqrt{-3})$.

Chapter 2

p-adic Numbers

The p-adic numbers were introduced by the mathematician Kurt Hensel[1] at the beginning of the twentieth century and have achieved an important role in number theory. As for their construction, on the one hand Hensel defined the p-adic numbers by first expressing the p-adic integers as formal series which constituted the projective limit that would be the ring of p-adic integers $\mathbb{Z}_p$ and the p-adics numbers its field of fractions. On the other hand, the mathematician J. Kürschak[2] proposed to view p-adic numbers analogously to the real numbers, so as a completion[3] of $\mathbb{Q}$ replacing the usual[4] by a new *p-adic* absolute value. In this chapter we are going to introduce the Kürschak's definition of the p-adic numbers since this construction helps to understand better idèles in the following chapter.

2.1 Construction

For the rest of this chapter we fix a prime number p.

Definition 2.1. Given a field K an *absolute value* or *multiplicative valuation* of the field is a map

$$|\ |\ :\ K \longrightarrow \mathbb{R}$$

such that given $x, y \in K$ the following properties verify

(i) $|x| \geqslant 0$, and $|x| = 0$ if and only if $x = 0$,

(ii) $|xy| = |x||y|$,

(iii) $|x + y| \leqslant |x| + |y|$ (triangle inequality)

[1] Kurt Hensel (1861-1941) a German mathematician also know for the Hensel's lemma.

[2] Jozsef Kürschak (1864 - 1933) a Hungarian mathematician the creator of the theory of valuations

[3] The definition of completion will be given in this chapter.

[4] The usual absolute value $|\ |$ is defined by

$$|x| = \begin{cases} x & \text{if } x \geqslant 0 \\ -x & \text{if } x < 0; \end{cases}$$

(iii') $|x+y| \leqslant \max\{|x|,|y|\}$ (strong triangle inequality)

We say that an absolute value verifying (i), (ii), (iii) is *archimedean*. While an absolute value that verifies (i), (ii), (iii') is called *non-archimedean*.

Remark 2.2. In particular, the strong triangle inequality implies the triangle inequality.

Definition 2.3. Given a field K and an absolute value $|\ |$ of the field, a *distance d* over K is induced by the valuation and is defined by

$$d(x,y) = |x-y|,\ \forall x,y \in K$$

And so the previous distance will make K into a metric space.
For the construction of the p-adic numbers the p-adic absolute value is used.

Definition 2.4. The *p-adic absolute value* is given by

$$\begin{aligned} |\ |_p\ :\ \mathbb{Q} &\longrightarrow \mathbb{R} \\ a &\longmapsto p^{-v_p(a)} \end{aligned}$$

where $v_p(a)$ denotes the p-adic exponential valuation.

Definition 2.5. The map v_p is called the *p-adic exponential valuation*, which we will refer to as p-adic valuation. Given $a = \frac{b}{c} \in \mathbb{Q}$ with $b, c \in \mathbb{Z}$ with $c \neq 0$ which can be expressed as $a = p^n \frac{b'}{c'}$ with b', c' coprime to p, the v_p it is the map

$$\begin{aligned} v_p :\ \mathbb{Q} &\longrightarrow \mathbb{Z} \cup \{\infty\} \\ a &\longmapsto n \end{aligned}$$

The p-adic valuation satisfies the following properties

(1) $v_p(a) = \infty$ if and only if $a = 0$

(2) $v_p(ab) = v_p(a) + v_p(b)$

(3) $v_p(a+b) \geqslant \min\{v_p(a), v_p(b)\}$

Example 2.6.

- An example of archimedean absolute value, is the absolute value at infinity denoted by $|\ |_\infty$. This absolute value is defined by

$$|x| = \begin{cases} x & \text{if } x \geqslant 0 \\ -x & \text{if } x < 0; \end{cases}$$

  that induces metric $d(x,y) = |x-y|$, which is the metric used to obtain the set of real numbers as a completion of $\mathbb{Q}$.

- The p-adic absolute value, $|\ |_p$, is an example of nonarchimedean valuation.

Definition 2.7. Two absolute values on a field K are *equivalent* if they define the same topology on K.

Theorem 2.8 (Ostrowski). *Every non-trivial multiplicative valuation of $\mathbb{Q}$ is equivalent to $|\ |_p$ for some prime p or to $|\ |_\infty$.*

Proof. See [4]. Chapter II.3, Proposition (3.7) □

Remark 2.9. The theorem states that every archimedean valuations of $\mathbb{Q}$ is equivalent to $|\ |_\infty$, while a nonarchimedean valuation is equivalent to $|\ |_p$ for some p prime. And so over $\mathbb{Q}$ we find the trivial absolute value, the infinite absolute value and the p-adic absolute value.

Remark 2.10. The rational numbers with the p-adic absolute value form the p-adic metric space.

Proposition 2.11 (Product Formula). *For any $a \in \mathbb{Q}^\times$ we have*

$$\prod_p |a|_p = 1$$

where p varies over all prime numbers as well as ∞.

Proof. Take the prime factorization of $a \in \mathbb{Q}^\times$

$$a = \pm \prod_{p \neq \infty} p^{v_p}$$

clearly for a rational number we have that $\frac{a}{|a|_\infty} = \pm 1$ and by the definition given of the p-adic valuation the exponent v_p coincides with $v_p(a)$ for all primes p. And so we can rewrite the equation as

$$a = \frac{a}{|a|_\infty} \prod_{p \neq \infty} p^{v_p(a)}$$

which is equivalent to

$$a = a|a|_\infty \prod_{p \neq \infty} p^{-v_p(a)}$$

so indeed when using cancellation and keeping in mind that for a fixed p by definition of the p-adic absolute value $p^{-v_p(a)} = |a|_p$ and so one gets that $\prod_p |a|_p = 1$. □

We move on to construct the p-adic numbers by completing the $\mathbb{Q}$.

Definition 2.12. A sequence $(x_n) \in K$ is called a *Cauchy sequence* with respect the absolute value $|\ |$ if for every $\epsilon > 0$ there exists a positive integer n_0 such that $|x_n - x_m| < \epsilon$, for all $m, n \geqslant n_0$

Definition 2.13. A field K with an absolute value $|\ |$ is *complete* if every Cauchy sequence $(x_n)_{n \in \mathbb{N}}$ converges to an element $a \in K$.

Theorem 2.14. *The field $\mathbb{Q}$ is not complete with respect to any of its nontrivial absolute value.*

Before we can prove the theorem we need to introduce the following result.

Lemma 2.15. *A sequence (x_n) of rational numbers is Cauchy with respect to a non-archimedean absolute value $|\ |$ if and only if*

$$\lim_{n\longrightarrow\infty} |x_{n+1} - x_n| = 0$$

Proof. First of all we suppose that(x_n) is a Cauchy sequence then for all $\epsilon > 0$ there exists $n_0 \in \mathbb{N}$ such that for all $n, m \geqslant n_0$ we have that $|x_m - x_n| < \epsilon$. Then we define m to be such that $m = n + 1$ and so for all $\epsilon > 0$ there exists $n_0 \in \mathbb{N}$ such that for all $n \geqslant n_0$ we have that $|x_{n+1} - x_n| < \epsilon$. Hence, $\lim_{n\longrightarrow\infty} |x_{n+1} - x_n| = 0$ just like we wanted to see.
As for the second implication, suppose that $\lim_{n\longrightarrow\infty} |x_{n+1} - x_n| = 0$, i.e. for all $\epsilon > 0$ there exist $n_0 \in \mathbb{N}$ such that for all $n \geqslant n_0$, $|x_{n+1} - x_n| < \epsilon$. Take $m > n \geqslant n_0$, then

$$\begin{aligned} |x_m - x_n| &= |x_m - x_{m-1} + x_{m-1} - x_{m-2} + \cdots + x_{n+1} - x_n| \\ &\leqslant \max\{|x_{n+r} - x_{n+r-1}|, \ldots, |x_{n+1} - x_n|\} < \epsilon \end{aligned}$$

where in the former inequality we have used that the absolute value is non-archimedean and in the last the original hypothesis. □

Proof theorem 2.14. According to Ostrowski's Theorem 2.8 we need to see that $\mathbb{Q}$ is not complete with respect $|\ |_\infty$ and p-adic absolute value.
We start with the absolute value at infinity $|\ |_\infty$. Take f_n to be the n-th Fibonacci number with $n \in \mathbb{N}$. We define a sequence (a_n) with $n \in \mathbb{N}$

$$a_n := \frac{f_n}{f_{n-1}}$$

where $f_0 = 0$, $f_1 = 1$ and $f_n = f_{n-1} + f_{n-2}$, $n > 1$. Let's verify that it is a Cauchy sequence. Given $m, n \in \mathbb{N}$ with $m > n$ and using the triangle inequality

$$|a_m - a_n| = |a_m - a_{m-1} + a_{m+1} - a_{m-2} + \cdots a_{n+1} - a_n| \leqslant \sum_{k=n}^{m-1} |a_{k+1} - a_k|$$

And so in order to see that (a_n) is Cauchy we first need to bound properly $|a_{n+1} - a_n|$.

$$\begin{aligned} |a_{n+1} - a_n| &= \left|\frac{f_{n+1}f_{n-1} - f_n^2}{f_n f_{n-1}}\right| \\ &= \left|\frac{f_n f_{n-1} + f_{n-1}f_{n-1} - f_n f_{n-1} - f_n f_{n-2}}{f_{n-1}f_{n-1} + f_{n-1}f_{n-3}}\right| \end{aligned}$$

As the Fibonacci sequence is increasing then $f_{n-1}^2 + f_{n-1}f_{n-2} > 2f_{n-1}f_{n-2}$ and we can bound $|a_{n+1} - a_n|$ in the following way,

$$|a_{n+1} - a_n| < \left|\frac{f_{n-1}^2 - f_n f_{n-2}}{2f_{n-1}f_{n-2}}\right| = \frac{1}{2}\left|\frac{f_n}{f_{n-1}} - \frac{f_{n-1}}{f_{n-2}}\right| = \frac{1}{2}|a_n - a_{n-1}|.$$

Using induction we see that

$$|a_{n+1} - a_n| < \left(\frac{1}{2}\right)^{n-2}\left|\frac{f_3}{f_2} - \frac{f_2}{f_1}\right| = \left(\frac{1}{2}\right)^{n-2}$$

Therefore we have that

$$|a_m - a_n| \leqslant \sum_{k=n}^{m-1} |a_{k+1} - a_k| \leqslant \sum_{k=0}^{m-n-1} |a_{n+k+1} - a_{n+k}|$$

and so using that we get a geometric series

$$|a_m - a_n| < \sum_{k=0}^{m-n-1} (1/2)^{n+k-2} = \left(\frac{1}{2}\right)^{n-2} \frac{1 - \left(\frac{1}{2}\right)^{m-n}}{1 - \frac{1}{2}} \leqslant \frac{1}{2^{n-2}}$$

And when $n \to \infty$ and since $m - n \in \mathbb{N}$ the right hand side converges to 0 and so the (a_n) is a Cauchy sequence. Moreover (a_n) converges to $\frac{1+\sqrt{5}}{2}$. And so (a_n) is a Cauchy sequence that doesn't convert in $\mathbb{Q}$. So $\mathbb{Q}$ isn't complete with respect to the infinite absolute value.

In case of a p-adic absolute value we will do the same, construct a Cauchy sequence in $\mathbb{Q}$ which doesn't have a limit in $\mathbb{Q}$ with respect to this absolute value. It will be a sequence of solutions modulo p^n of an equation that has no solutions in $\mathbb{Q}$.
We suppose $p \neq 2$. Choose an integer a such that

- a is not a square in $\mathbb{Q}$;
- p does not divide a;
- a is a quadratic residue modulo p.

We now move on to construct a Cauchy sequence with respect to $|\ |_p$.

- Choose x_0 such that $x_0^2 \equiv a \mod p$
- Choose x_1 so that $x_1 \equiv x_0 \mod p$ and $x_1^2 \equiv a \mod p^2$ which we know exists by Hensel's Lemma.
- In general, we choose x_n to be such that

$$x_n \equiv x_{n-1} \mod p^n \quad \text{and} \quad x_n^2 \equiv a \mod p^{n+1}$$

We need to verify that it is indeed a Cauchy sequence. From the construction it is clear that

$$|x_{n+1} - x_n|_p = |bp^{n+1}|_p \leqslant p^{-(n+1)} \underset{n \longrightarrow \infty}{\to} 0, \text{ for some } b$$

Which shows that it is a Cauchy sequence by Lemma 2.15. Moreover

$$|x_n^2 - a|_p = |cp^{n+1}|_p \leqslant p^{-(n+1)} \underset{n \longrightarrow \infty}{\to} 0, \text{ for some } c$$

and so if the limit would be square root of a, which isn't in $\mathbb{Q}$ and so we have found a Cauchy sequence which is not complete with respect to $|\ |_p$.
As for the case when $p = 2$ can be done in a similar way using cubic roots instead of squares. So we can conclude that $\mathbb{Q}$ is not complete with respect p-adic absolute value. $\square$

Remark 2.16. Since $\mathbb{Q}$ is not complete with respect any nontrivial absolute value it makes sense to talk about its completion which will be different from $\mathbb{Q}$ itself.

Just as in the set of real numbers, here we can associate equivalence classes to Cauchy sequences. We will define $\mathbb{Q}_p$ to be the set of equivalence classes of Cauchy sequences. First of all, we will denote by C the set of Cauchy sequences of elements of $\mathbb{Q}$ with respect to the metric induced by a p-adic absolute value.

Proposition 2.17. *C is a commutative ring with the operations defined component-wise, i.e. given two sequences $(x_n), (y_n)$ we have*

$$(x_n) + (y_n) := (x_n + y_n)$$
$$(x_n)(y_n) := (x_n y_n)$$

Proof. The commutative ring axioms follow clearly by the definition. But we do want to see that the sequences obtained are Cauchy. So we want to see that $(x_n + y_n)$ is a Cauchy sequence. First of all we have that (x_n) and (y_n) are Cauchy sequences in $\mathbb{Q}$ so for every $\epsilon > 0$ there exists $n_1, n_2 \in \mathbb{N}$ such that for all $n, m \geqslant n_1$, we have $|x_n - x_m|_p < \epsilon$ and for all $n, m \geqslant n_2$, $|y_n - y_m|_p < \epsilon$. Therefore for all $n, m \geqslant n_0 := \max\{n_1, n_2\}$

$$|x_n + y_n - x_m - y_m|_p \leqslant \max\{|x_n - x_m|_p, |y_n - y_m|_p\} < \epsilon.$$

The additive identity element is defined as the constant sequence (0).
The additive inverses $-(x_n)$ is the sequence $(-x_n)$.
As for the multiplication, bare in mind that every Cauchy sequence is bounded, so there exists A and B such that for all $n \in \mathbb{N}$, we have $|x_n|_p < A$ and $|y_n|_p < B$ and $C = max\{A, B, 1\}$. For the Cauchy sequences (x_n) and (y_n) we suppose that $|x_n - x_m|_p < \epsilon/C$ and also $|y_n - y_m|_p < \epsilon/C$. And so we want to see that indeed $(x_n y_n)$ is Cauchy. Given $n, m \geqslant n_0$,

$$\begin{aligned} |x_n y_n - x_m y_m|_p &\leqslant |x_n y_n - x_n y_m + x_n y_m - x_m y_m|_p \\ &\leqslant \max\{|x_n(y_n - y_m)|_p, |(x_n - x_m)y_m|_p\} < C\frac{\epsilon}{C} = \epsilon \end{aligned}$$

and it is a Cauchy sequence.
The multiplicative identity element is define as the constant sequence (1).
The commutative property and the left out details are easy to check. And so C is a commutative ring. □

Remark 2.18. C is not a field since it has zero-divisors.

Definition 2.19. A sequence (x_n) in $\mathbb{Q}$ is called a *nullsequence* with respect to p-adic absolute value if $|x_n|_p$ is a sequence converging to 0.

Now we want to identify the Cauchy sequences with the same limit. Denote $N \subset C$ the ideal of nullsequences.

Proposition 2.20. *N is a maximal ideal of C.*

Proof. First we want to see that indeed N is an ideal of C.
Suppose $(x_n), (y_n) \in N$, so we have that for all $\epsilon > 0$ there exists $n_0 \in \mathbb{N}$ such that for all $n \geqslant n_0$, $|x_n|_p < \epsilon$, hence for all $n, m \geqslant n_0$

$$|x_n - x_m|_p \leqslant \max\{|x_n|_p, |x_m|_p\} \leqslant \epsilon$$

And so (x_n) is a Cauchy sequence with the multiplication defined component-wise and so it is a subgroup of C. Now if we take another sequence $(y_n) \in C$, then it is clear that $(x_n)(y_n) = (x_n y_n)$ will be nullsequence since $|x_n y_n|_p = |x_n|_p |y_n|_p$ and (y_n) is bounded. So we can see that N is an ideal of C.

Now suppose I the ideal generated by (x_n) and N, $(x_n) \notin N$. We want to prove that in this case I ought to be all of C. It is enough to show that I contain the unit element (1), since any ideal containing the unit element must be the whole ring.
Since (x_n) isn't nullsequence, then there exists $c > 0$ such that for all $n_1 \in \mathbb{N}$ there exists $n \geqslant n_1$, $|x_n|_p \geqslant c > 0$. Moreover we have that it is a Cauchy sequence, and so for the given c there exists $n_2 \in \mathbb{N}$ such that for all $m, n \geqslant n_2$, $|x_n - x_m|_p < \epsilon$. Suppose $n_0 = \max\{n_1, n_0\}$ and that $m > n \geqslant n_0$,

$$|x_n|_p \leqslant |x_n - x_m + x_m|_p \leqslant \max\{|x_n - x_m|_p, |x_m|_p\} = |x_m|_p$$

due to the fact that $|x_n - x_m|_p < \epsilon$ while $|x_m|_p \geqslant c > 0$, we have that

$$|x_m|_p \geqslant |x_n|_p \geqslant c > 0$$

So far we have proved that there exists $c > 0$ and an integer n_0 such that for all $n \geqslant n_0$, $|x_n|_p \geqslant c > 0$, so $x_n \neq 0$ whenever $n \geqslant n_0$. We can define a new sequence (y_n)

$$y_n = \begin{cases} 0 & \text{if } n < n_0 \\ \frac{1}{x_n} & \text{if } n \geqslant n_0 \end{cases}$$

Let $n \geqslant n_0$

$$|y_{n+1} - y_n|_p = \frac{|x_{n+1} - x_n|_p}{|x_{n+1} x_n|_p} \geqslant \frac{|x_{n+1} - x_n|_p}{c^2} \xrightarrow[n \to \infty]{} 0$$

by lemma 2.15 this proves that $(y_n) \in C$
Notice that

$$x_n y_n = \begin{cases} 0 & \text{if } n < n_0 \\ 1 & \text{if } n \geqslant n_0 \end{cases}$$

hence $(1) - (x_n)(y_n) \in N$, and (1) belongs to I. We can conclude that N is a maximal ideal in C. □

Definition 2.21. The p-adic numbers is the set of equivalence classes of Cauchy sequences

$$\mathbb{Q}_p := {}^{C}/_{N}$$

Corollary 2.22. *$\mathbb{Q}_p$ is a field.*

Proof. A quotient of a ring by a maximal ideal gives a field. □

Remark 2.23. And the inverse of elements of the field $\{x_n\}^{-1}$ will be $\{x_n^{-1}\}$, and whenever $x_n = 0$ it is easy to see that we can replace it by $x_n^{'} = p^n$ blinding an equivalent Cauchy sequence, and so that every Cauchy sequence is equivalent to one with no zero terms.

To any element $a \in \mathbb{Q}$ we associate the constant sequence (a), which gives an embedding of $\mathbb{Q}$ into $\mathbb{Q}_p$.

As for the p-adic absolute value $|\ |_p$, it extends to $\mathbb{Q}_p$ as follows

$$\begin{aligned} |\ |_p :\ \mathbb{Q}_p = C/N &\longrightarrow \mathbb{R} \\ x &\longmapsto \lim_{n\longrightarrow\infty} |x_n|_p \end{aligned}$$

where $x = \{x_n\} \mod m \in C/N$. We want to check that in fact the limit does exists.

- If $x = 0$, then by definition $\lim_{n\longrightarrow\infty} |x_n|_p = 0$.
- If $x \neq 0$, then there exist $\epsilon > 0$ and $n_0 \in \mathbb{N}$ such that for all $n > n_1$ $|x_n|_p \leqslant \epsilon$. And since the given sequence is Cauchy, there also exists n_2 such that for all $m, n \geqslant n_2$, $|x_n - x_m|_p < \epsilon$. So if we set $n_0 = \max\{n_1, n_2\}$ then once has that for all $m, n \geqslant n_0$, $|x_n - x_m|_p < \max\{|x_n|_p, |x_m|_p\}$ and by the non-archimedean property that all triangles are isosceles $|x_n|_p = |x_m|_p$. So it is eventually stationary.

Moreover as any p-adic nullsequence $\{y_n\} \in N$ satisfies that $\lim_{n\to 0} |y_n|_p = 0$ then the limit is independent of the choice of the sequence within its class $\mod m$.

Remark 2.24. We do get that for all $x \in \mathbb{Q}_p$, $|x|_p = p^{-v_p(x)}$, where we extend $v_p(x)$ to $\mathbb{Q}_p$ in the following way[5]. Given $x = (x_n) \in \mathbb{Q}_p$, $x_n \neq 0$

$$\begin{aligned} v_p :\ \mathbb{Q}_p &\longrightarrow \mathbb{Z} \cup \{\infty\} \\ x &\longmapsto \lim_{n\longrightarrow\infty} v_p(x_n) \end{aligned}$$

where

$$v_p(x_n) = -log_p|x_n|_p$$

Proposition 2.25. *The field $\mathbb{Q}_p$ of p-adic numbers is complete with respect to $|\ |_p$.*

Proof. To prove that the field $\mathbb{Q}_p$ of p-adic numbers is complete with respect to $|\ |_p$. We will see that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. And so we want to see that for every point $x \in \mathbb{Q}_p$ any neighbourhood of x contains at least one element of $\mathbb{Q}$.
Let x be a p-adic number,which we can think of as a succession. And we want to see that if we fix $\epsilon > 0$, we want to see that the neighbourhood that is a ball $B(x, \epsilon) = \{y \in \mathbb{Q}_p \ :\ |x - y|_p < \epsilon\}$ contains a rational number or a constant succession of rational numbers.

[5]Those interested can find more details in [4].

To prove the desired result, take a Cauchy sequence of rational numbers $x = (a_i)$. Since it s a Cauchy sequence, for the previously fixed ϵ, we now that there exists n_0 such that $|a_n - a_m|_p < \epsilon$, for all $m, n > n_0$.
Now we denote $q = a_{n_0}$ and we want to check that this rational number is going to be in the neighbourhood of x. And so we have a loot at the distance between the two points,

$$|x - q|_p := \lim_{i\to\infty} |a_i - q|_p = \lim_{i\to\infty} |a_i - a_{n_0}|_p < \epsilon$$

Even thought we do not know the concrete value of the limit, we do not that the distance between the two points is smaller than ϵ and so $q \in B(x, 1)$. And since we have proved that for every point $x \in \mathbb{Q}_p$ any neighbourhood of x contains at least one element of $\mathbb{Q}$, $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.
And so every point in $\mathbb{Q}_p$ is either an element in $\mathbb{Q}$ or an accumulation point of $\mathbb{Q}$.Therefore, the field of p-adic numbers is complete with respect to $|\ |_p$. □

So we have constructed the p-adic numbers as an extension of $\mathbb{Q}$.

2.2 The field of p-adic numbers

Having constructed the p-adic numbers, in this section we will see some results related to them.

Proposition 2.26. *The set*

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p \ : \ |x|_p \leqslant 1\}$$

is a subring of $\mathbb{Q}_p$. It is the closure with respect to $|\ |_p$ of the ring $\mathbb{Z}$ in the field $\mathbb{Q}_p$.

Proof. The fact that $\mathbb{Z}_p$ is closed under addition and multiplication follows from

$$|x + y|_p \leqslant \max\{|x|_p, |y|_p\} \text{ and } |xy|_p = |x|_p|y|_p$$

Let $\{x_n\}$ be a Cauchy sequence in $\mathbb{Z}$ and $x = \lim_{n\to\infty} x_n$, then $|x_n|_p \leqslant 1$ implies $|x|_p \leqslant 1$, therefor $x \in \mathbb{Z}_p$. On the other hand suppose , let $x = \lim_{n\to\infty} x_n \in \mathbb{Z}_p$, for a Cauchy sequence $\{x_n\} \in \mathbb{Q}$. And one has $|x|_p = |x_n|_p \leqslant 1$, for $n \geqslant n_0$, i.e. $x_n = a_n$, with $a_n, b_n \in \mathbb{Z}$, $(b_n, p) = 1$. Choosing for each $n \geqslant n_0$ a solution $y_n \in \mathbb{Z}$ of the congruence $b_n y_n \equiv a_n \mod \frac{1}{p_n}$ we have $|x_n - y_n|_p \geqslant p_n$, and therefore $x = \lim_{n\to\infty} y_n$, so that x belongs to the closure of $\mathbb{Z}$. □

Clearly the group of units of $\mathbb{Z}_p$ is

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p \ : \ |x|_p = 1\}$$

Moreover, if $v_p(x) = n \in \mathbb{Z}$, then $v_p(xp^{-n}) = 0$, hence $|xp^{-n}|_p = 1$, and so $u = xp^{-n} \in \mathbb{Z}_p^\times$

Remark 2.27. Every element $x \in \mathbb{Q}_p^\times$ admits a unique representation

$$x = p^n u \text{ with } n \in \mathbb{Z} \text{ and } u \in \mathbb{Z}_p^\times$$

And so me have an isomoprhism

$$\begin{aligned} \theta \ : \ \mathbb{Q}_p^\times &\longrightarrow \mathbb{Z}_p^\times \times p^{\mathbb{Z}} \\ x &\longmapsto (u, p^n) \end{aligned}$$

Proposition 2.28. *The nonzero ideals of the ring $\mathbb{Z}_p$ are the principal deals*

$$p^n\mathbb{Z}_p = \{x \in \mathbb{Q}_p \ : \ v_p(x) \geqslant n\}$$

with $n \geqslant 0$, and we have

$$\mathbb{Z}_p \Big/ p^n\mathbb{Z}_p \cong \mathbb{Z} \Big/ p^n\mathbb{Z}$$

Proof. Suppose $\mathfrak{a} \neq (0)$ an ideal of $\mathbb{Z}_p$ and $x = p^m u, \ u \in \mathbb{Z}_p^\times$, an element of $\mathfrak{a}$ with smallest possible m (since $|x|_p \leqslant 1$, one has $m \geqslant 0$). Then $\mathfrak{a} = p^m\mathbb{Z}_p$, because if we take $y = p^n u' \in \mathfrak{a}, \ u' \in \mathbb{Z}_p^\times$, implies $n \geqslant m$, hence $y = (p^{n-m}u')p^m \in p^m\mathbb{Z}_p$.
The homomorphism

$$\begin{aligned} \mathbb{Z} &\longrightarrow \mathbb{Z}_p \Big/ p^n\mathbb{Z}_p \\ a &\longmapsto a \mod p^n\mathbb{Z}_p \end{aligned}$$

has kernel $p^n\mathbb{Z}$ and is surjective. We can see that indeed, given $x \in \mathbb{Z}_p$, there exists by Proposition 2.26 an $a \in \mathbb{Z}$ such that

$$|x - a|_p \leqslant \frac{1}{p^n}$$

i.e., $v_p(x - a) \geqslant n$, therefore $x - a \in p^n\mathbb{Z}_p$, therefore $x \equiv a \mod p^n\mathbb{Z}_p$. So we obtain an isomorphism

$$\mathbb{Z}_p \Big/ p^n\mathbb{Z}_p \cong \mathbb{Z} \Big/ p^n\mathbb{Z}$$

□

Chapter 3

Hecke Characters

Erich Hecke[1] introduced Hecke Character, also known as Größencharakter, as a generalization of a Dirichlet character in order to extend L-functions to arbitrary number fields, not only rational numbers. There are two possible ways to define Hecke Character, the classical one given originally by Hecke uses ideals while in the second one the Hecke character is defined by using idèles. There is a relation between the two definitions that can be expressed precisely. In our case the definition used is based on idèles, therefore before moving on to the Hecke characters the necessarily theory on idèles will be introduced.

In analogy to the p-adic numbers with p being a primer number, introduced in the previous chapter, we can talk about the $\mathfrak{p}$-adic numbers with $\mathfrak{p}$ being a prime of an algebraic number field K.

Definition 3.1. A *prime* or *place* $\mathfrak{p}$ of a number field K is a class of equivalent valuations of K. The non-archimedean equivalence classes are called *finite* primes and the archimedean ones *infinite* primes.

Since a number field is a finite algebraic extensions of $\mathbb{Q}$ if we have an archimedean valuation v of $\mathbb{Q}$, when we want to extend we associate some embeddings $\tau : K \longrightarrow \mathbb{C}$ to it[2], and this embedding helps us obtain the infinite places. We say that τ is a real embedding if $Im\tau = \mathbb{R}$, otherwise it is a complex embedding.
When referring to an infinite place we can talk about

- *Real primes*, given by embeddings $\tau : K \longrightarrow \mathbb{R}$. Denoted as $\mathfrak{p}|\infty$.
- *Complex primes*, given by the pair of complex conjugate non-real embedding $K \longrightarrow \mathbb{C}$. Denoted as $\mathfrak{p} \nmid \infty$.

To each $\mathfrak{p}$ of K we associate a canonical homomorphism

$$v_{\mathfrak{p}} : K^{\times} \longrightarrow \mathbb{R}$$

[1] Erich Hecke (1887 – 1947), German mathematician. Hecke devoted most of his research to the theory of modular forms.

[2] For more details see [4] Chapter II.8 , Extension Theorem 8.1

therefore can talk about the completion $K_\mathfrak{p}$. On one hand, when $\mathfrak{p}$ is finite, $v_\mathfrak{p}$ is the $\mathfrak{p}$-adic exponential valuation with the condition $v_\mathfrak{p}(K^\times) = \mathbb{Z}$. On the other hand, if $\mathfrak{p}$ is infinite, then $v_\mathfrak{p}(a) = -\log|\tau a|$ where $\tau : K \longrightarrow \mathbb{R}$ is an embedding that defines $\mathfrak{p}$.

Proposition 3.2. *When we have $\mathfrak{p}$ a finite prime, then every element $x \in K_\mathfrak{p}^\times$ admits a unique representation as*

$$x = u\pi^n,\ u \in \mathcal{O}_\mathfrak{p}^\times,\ n \in \mathbb{Z}$$

with $\pi \in \mathcal{O}_\mathfrak{p}$ such that $v_v(\pi) = 1$ is an uniformizing parameter. And so we have that

$$K_\mathfrak{p}^\mathbb{Z} \cong \mathcal{O}_\mathfrak{p}^\times \times \pi^\times$$

where $\pi^\mathbb{Z} = \{\pi^k : k \in \mathbb{Z}\}$.

Proof. For if $v_\mathfrak{p}(x) = n$, then $v_\mathfrak{p}(x\pi^{-n}) = 0$, hence $u = x\pi^{-n} \in \mathcal{O}_{\mathfrak{p}^\times}$. □

We are going to define idèles to be the restricted product of $K_\mathfrak{p}$, where the restricted product refers to the following

Definition 3.3. *Given I indexing set and a finite subset $S \subset I$. Suppose G_i locally compact group for all $i \in I$ and that for all $i \in I \setminus S$ we have $K_i \subset G_i$ an open compact subgroup. Then the restricted product with respect to the $K_i \subset G_i$*

$$\overline{\prod_i} G_i = \{(g_i)_{i\in I} : g_i \in K_i \text{ for all but finitely many } i \in I\} \leqslant \prod_{i\in I} G_i$$

And so we can now properly define an idèle.

Definition 3.4. Given a number field K we define an *idèle* as a family $\alpha = (\alpha_\mathfrak{p})$ of elements $\alpha_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^\times \subseteq K_\mathfrak{p}$ for almost all $\mathfrak{p} \in K$.

Definition 3.5. The idèles form the *idèle group* I_K that is a restricted product of the $K_\mathfrak{p}^\times$ with respect to the units of the ring of integers $\mathcal{O}_\mathfrak{p}^\times \subseteq K_\mathfrak{p}^\times$

$$I_K = \overline{\prod_\mathfrak{p}} K_\mathfrak{p}^\times = \{(\alpha_\mathfrak{p}) : \alpha_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^\times \text{ for all but finitely many } \mathfrak{p}\}$$

with addition and multiplication defined componentwise.

Proposition 3.6. *Given a number field K and a place $\mathfrak{p}$*

$$K\mathfrak{p}^\times \cong \begin{cases} \mathbb{R}^\times & \text{if } \mathfrak{p} \text{ infinite real} \\ \mathbb{C}^\times & \text{if } \mathfrak{p} \text{ infinite complex} \\ \mathbb{Z} \times \mathcal{O}^\times & \text{if } \mathfrak{p} \text{ finite} \end{cases}$$

Proof. When introducing infinite places , We have mentioned that they are obtained using an embedding $\tau : k \longrightarrow \mathbb{C}$. In case of a real embedding, i.e. $Im\tau = \mathbb{R}$, we have that

$$\mathbb{Q} \subseteq K \subseteq \mathbb{R}$$

and so if we complete each of the previous fields, we obtain

$$\mathbb{R} \subseteq K_{\mathfrak{p}} \subseteq \mathbb{R}$$

and so we get that $K_{\mathfrak{p}}^{\times} \cong \mathbb{R}$. On the other hand, when we have a complex embedding and its completion , we get

$$\mathbb{Q} \subseteq K \subseteq \mathbb{C}$$
$$\mathbb{R} \subseteq K_{\mathfrak{p}} \subseteq \mathbb{C}$$

and since in this case $Im\tau \neq \mathbb{R}$, we can conclude that $K_{\mathfrak{p}}^{\times} \cong \mathbb{C}$.
If we have that $\mathfrak{p}$ is finite prime, then using Proposition 3.2 we have that

$$K_{\mathfrak{p}}^{\times} \cong \mathcal{O}_{\mathfrak{p}}^{\times} \times \pi^{\mathbb{Z}}$$

And clearly $\pi^{\mathbb{Z}} \cong \mathbb{Z}$. So we have that $K_{\mathfrak{p}}^{\times} \cong \mathcal{O}_{\mathfrak{p}}^{\times} \times \mathbb{Z}$ □

For every finite set S of primes, I_K contains S-idèles which is the subgroup

$$I_K^S = \prod_{p \in S} K_{\mathfrak{p}^{\times}} \times \prod_{p \notin S} U_{\mathfrak{p}}$$

where $U_{\mathfrak{p}} = K_{\mathfrak{p}^{\times}}$ for $\mathfrak{p}$ infinite complex, and $U_{\mathfrak{p}} = \mathbb{R}_{+}^{\times}$ for $\mathfrak{p}$ infinite real. Obviously if S varies over all finite sets of primes of K we have that

$$I_K = \bigcup_S I_K^S$$

The group $K^{\times}$ is embedded diagonally in I_K. That is, since $K \subseteq K_{\mathfrak{p}}$, then we have

$$\begin{aligned} K^{\times} &\longrightarrow I_K \\ x &\longmapsto (x_{\mathfrak{q}}) = (x) \end{aligned}$$

where (x) denotes the constant sequence. Contrary, the group $K_{\mathfrak{p}}$ is embedded in one component:

$$\begin{aligned} K_{\mathfrak{p}}^{\times} &\longrightarrow I_K \\ x &\longmapsto (x_{\mathfrak{q}}) = \begin{cases} x_{\mathfrak{q}} = x_{\mathfrak{p}} & \text{if } \mathfrak{p} = \mathfrak{q} \\ x_{\mathfrak{q}} = 1 & \text{if } \mathfrak{p} \neq \mathfrak{q} \end{cases} \end{aligned}$$

It is easy to check that it is a group morphism and to see that it is well-defined we have to verify that $(x_{\mathfrak{q}})$ is an idèle. Since all but one component are 1, and so we have that $(x_{\mathfrak{q}}) \in \mathcal{O}_{\mathfrak{p}}^{\times}$ so it is an idèle.

Remark 3.7. $K^{\times}$ is a subgroup of I_K and its elements are the so-called *principal idèles* in I_K.

Definition 3.8. Given the idèle group I_K and its subgroup of principal idèles $K^{\times}$, the quotient group

$$C_K = I_K / K^{\times}$$

is the *idèle class group* of K.

Having seen the necessary theory, we can now define a Hecke character.
First we fix a number field K. As we have mentioned we want to define the Hecke Character from an idèlic point of view.

Definition 3.9. $C = {}^{I_K}/_{K^\times}$ is the idèle class group of K and we define a *Hecke character* of K as a character of the idèle class group and so as a continuous homomorphism

$$\mathcal{X} \ : \ I_K \longrightarrow \mathbb{C}^\times$$

of the idèle group I such that $\mathcal{X}(K^\times) = 1$

Chapter 4

Conclusions

Having seen some example of how to find out how many points there are of an elliptic curve E over a finite field $\mathbb{F}_q$, and even though there are different computational algorithm that can be applied in order to work it out if we want to do it ourselves it is not an easy road to take.
We have already seen that Gauss' theorem gives us the number of projective solutions that there are of a concrete elliptic curve with complex multiplication. As we have already seen its statement is,

Theorem 4.1 (Gauss). *Let p be a prime and M_p the number of projective solutions to the equation*

$$x^3 + y^3 + z^3 = 0$$

with x, y, z in the field $\mathbb{F}_p$

- *If $p \not\equiv 1 \ (mod\ 3)$, then $M_p = p + 1$.*
- *If $p \equiv 1 \ (mod\ 3)$, then there are integers A and B such that*

$$4p = A^2 + 27B^2$$

A and B are unique up to changing their signs, and if we fix a sign of A so that $A \equiv 1 \ (mod\ 3)$, then

$$M_p = p + 1 + A$$

As already mentioned, the cubic in the theorem is an elliptic curve with complex multiplication, and so there might not yet be an easy way or a general formula to count the points of any elliptic curve over a finite field but this theorem was the first step to work concretely with the case of elliptic curves with complex multiplication.

There are results that in fact give the number of points of an elliptic curve with complex multiplication over a finite field. The idea behind this fact is that the L-functions associated to a Dirichlet character are representative for properties related to the arithmetic of number fields and the theory of numbers. Moreover, there is a further generalization of

L-functions by Artin and Hecke to Artin L-functions and Hecke L-functions associated to arithmetic general objects and number field.

This generalization has to do with the following observation. We get back to the Gauss theorem, we have seen that $x^3 + y^3 + z^3 = 0$ is an elliptic with complex multiplication and its endomorphism is the ring of integers $\mathcal{O} = \mathbb{Z}\left[(1+\sqrt{-3})/2\right]$ of $\mathbb{Q}(\sqrt{-3})$. Since we have that it has a class number one then we have that it is a principal ideal domain, and in fact a unique factorization domain. The prime numbers in $\mathcal{O}$ that are irreducible are those that verify that $p \not\equiv 1 \mod 3$. On the other hand, the prime numbers that verify that $p \equiv 1 \mod 3$ factorize in $\mathcal{O}$. And if we look on the statements in the Gauss theorem with this perspective.
First of all, in case that p is is irreducible in $\mathcal{O}$ then we have that $M_p = p + 1$. If p is not irreducible in $\mathcal{O}$, then $M_p = p + 1 + A$, where A is the real part of the factorization $4p = (A + 3B\sqrt{-3})(A - 3B\sqrt{-3})$.
And so using this idea as an approach to the Gauss theorem, there is a generalization of the Gauss theorem in order to compute the amount of points of an elliptic curve with complex multiplication over a finite field.
Concretely, let E an elliptic curve over $\mathbb{Q}$ with complex multiplication by $\mathcal{O}$ a ring of integers of an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-l})$. In case that p is irreducible in $\mathcal{O}$, then $p = A^2 + lB^2 = (A + B\sqrt{-l})(A - B\sqrt{-l})$ and the amount of points of E over a finite field $\mathbb{F}_p$ is $M_p = p + 1 + A$. Contrarily, if p is irreducible in the ring of integers $\mathcal{O}$ then there are $p + 1$ points in E over $\mathbb{F}_p$. Both Hecke characters and Hecke L-functions are important in the generalization of Gauss' theorem.

To every elliptic curve over $\mathbb{Q}$ with complex multiplication we can associate a Hecke character due to a decomposition phenomena. More precisely and in relation to the L-functions, if we think of these elliptic curves over $\mathbb{Q}$ as a mathematical objects then we can associate an L-function to the elliptic curves over $\mathbb{Q}$ containing information about M_p in a compact form for all p prime. If E has complex multiplication these L-functions can be decomposed into a sum of two "conjugated" elements, that correspond to a Hecke character each over an imaginary quadratic field K in a way that we will not explain.
It is really important to note that this phenomena only verifies for elliptic curves with complex multiplication, since in this case the study of the L-function is much easier.

A detailed study of the generalization of Gauss' theorem in case of elliptic curves over rational numbers with complex multiplication over an imaginary quadratic field was a motivation for this work. The theory and tools we have seen are a first small step into a much more deeper and rich theory, which is a possible further path of this dissertation.

Bibliography

[1] Fernando Q. Gouvêa, *p-adic Numbers. An Introduction*, Springer, 2nd edition (2003).

[2] Anthony W. Knapp, *Elliptic Curves*. Math Notes. 40 , Princeton University, (1992).

[3] Neal Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. Graduate Texts in Mathematics. 58 , Springer-Verlag (1977).

[4] Jürgen Neukirch, *Algebraic Numbre Theory.* Grundlehren der mathematischen Wissenschaften. 322, Berlin: Springer-Verlag (1999).

[5] Joseph H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. 151 , New York: Springer-Verlag (1994).

[6] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. 106 , Springer, 2nd edition (2009).

[7] Joseph. H. Silverman; John Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, 2nd printing (1994).

[8] Lawrence C. Washington. *Elliptic Curves: Number theory and cryptography*, Taylor and Francis Group, 2nd edition (2008).